SafeNet Authentication Client

Version 8.2 Revision A

User’s Guide

Copyright © 2012 SafeNet, Inc. All rights reserved.

All attempts have been made to make the information in this document complete and accurate.

SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet and SafeNet Authentication Manager are either registered with the U.S. Patent and Trademark Office or are trademarks of SafeNet, Inc., and its subsidiaries and affiliates, in the United States and other countries. All other trademarks referenced in this Manual are trademarks of their respective owners.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Date of publication: October 2012

Last update: Thursday, November 15, 2012 6:19 pm

Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact us directly at:

Telephone

You can call our help-desk 24 hours a day, seven days a week:
USA: 1-800-545-6608
International: +1-410-931-7520

Email

You can send a question to the technical support team at the following email address:
support@safenet-inc.com

Website

You can submit a question through the SafeNet Support portal:
http://c3.safenet-inc.com/secure.asp

Additional Documentation

The following SafeNet publications are available:

- SafeNet Authentication Client 8.2 Administrator’s Guide
- SafeNet Authentication Client 8.2 ReadMe

Table of Contents

1 Introduction

SafeNet Authentication Client enables token operations and the implementation of token PKI-based solutions.

In this chapter:

Overview

SafeNet Authentication Client is Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an internet transaction.

SafeNet Authentication Client provides easy-to-use configuration tools for users and administrators.

SafeNet Authentication Client Main Features

SafeNet Authentication Client incorporates features that were supported by previous releases of eToken PKI Client and SafeNet Borderless Security (BSec). It provides a unified middleware client for a variety of SafeNet smart cards, SafeNet iKey tokens, and SafeNet eToken devices.

Full backward compatibility means that customers who have been using eToken PKI Client or SafeNet Borderless Security Client (BSec) can continue to use deployed eToken and iKey devices.

What's New

SafeNet Authentication Client 8.2 offers the following new features:

- **Virtual Keyboard** - The Virtual Keyboard enables you to enter passwords without using the physical keyboard, providing protection against kernel level key loggers.
- **SafeNet eToken 7300** - SafeNet eToken 7300 is a certificate-based authentication solution that conveniently stores data and applications on up to 64GB of encrypted flash memory.

Supported Browsers

SAC 8.2 supports the following browsers:

- Firefox 5 and later
- Internet Explorer 7, 8, 9, 10
- Chrome version 14 and later, for authentication only (Does not support enrollment)

Supported Platforms

SAC 8.2 supports the following operating systems:

- Windows XP SP2, SP3 (32-bit, 64-bit)
- Windows Server 2003 SP2 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Vista SP2 (32-bit, 64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
- Windows Server 2012

NOTE
SAC 8.2 is compatible with Windows 7 (Submission ID 13329101) and Windows 8 (Submission ID 13329505) Logo program.

Supported Tokens

SafeNet Authentication Client 8.2 supports the following tokens:

- SafeNet eToken 7300
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 4100
- SafeNet eToken PRO
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard
- SafeNet eToken NG-OTP
- SafeNet eToken NG-Flash
- SafeNet eToken NG-Flash Anywhere
- SafeNet eToken Virtual Family
- SafeNet iKey: 2032, 2032u, 2032i
- SafeNet Smartcard: SC330, SC330u, SC330i
- SafeNet Smartcard SC400
- SafeNet iKey 4000

Supported Localizations

> **NOTE**
> Localizations are not supported in the BSec utility applications.

SafeNet Authentication Client 8.2 supports the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- English
- French (Canadian)
- French (European)
- German
- Hungarian
- Italian
- Japanese
- Korean
- Lithuanian
- Polish
- Portuguese (Brazilian)
- Romanian

- Russian
- Spanish
- Thai
- Vietnamese

2 SafeNet Authentication Client User Interfaces

This section describes the SafeNet Authentication Client user interfaces.

> **NOTE**
> If a customized version of the SafeNet Authentication Client is installed, the graphics you see may be different than those displayed in this guide.

In this chapter:

Overview of SafeNet Authentication Client User Interfaces

SafeNet Authentication Client provides two user interfaces:

- SafeNet Authentication Client Tray Icon
  - for quick access to many of the functions in the application
- SafeNet Authentication Client Tools
  - provides information about each connected token, including its identification and capabilities
  - has access to information stored on each connected token, such as keys and certificates
  - enables management of token content, such as password profiles

SafeNet Authentication Client Tray Icon

The SafeNet Authentication Client tray icon offers a shortcut menu to many of the application’s functions.

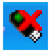
NOTE
To display the icon if it is hidden, see *Showing SafeNet Authentication Client Tray Icon* on page 162.

When SafeNet Authentication Client is closed, the tray icon is not displayed.

In the standard SafeNet Authentication Client installation, the tray icon is displayed as:

In the BSec UI compatible SafeNet Authentication Client installation, the tray icon is displayed as:

(token connected)

 (token disconnected)

Starting SafeNet Authentication Client

To start SafeNet Authentication Client:

- From the Windows taskbar, select **Start** > **Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client.**

Closing SafeNet Authentication Client

To close SafeNet Authentication Client:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Exit**.

Opening the Tray Menu

To access the shortcut menu from the SafeNet Authentication Client tray icon:

- Right-click the SafeNet Authentication Client tray icon.

SafeNet Authentication Client Tray Menu Functions

The following functions can be accessed quickly from the tray menu:

- **Explore Flash:** displayed when connecting the eToken 7300. Available only once you have logged on to flash. Once logged on, you will be able to open the folder to view files within the relevant drive.
- **Log On to Flash/Log off from Flash:** displayed when connecting the eToken 7300. Opens the *Password* window (if the SafeNet eToken 7300 is configured with a password protected Flash partition) and then the Windows AutoPlay window to access the SafeNet eToken 7300 Flash partition.
- **Change Token Password:** opens the *Change Password* window for the selected token.
- **Certificate Information:** opens the *Token Certificate Information* window.
- **Unlock Token:** opens the *Unlock Token* window.
- **Select Token:** allows you to select one of the connected tokens to be the active token. This function is available only when more than one token is connected.
- **Tools:** opens *SafeNet Authentication Client Tools*.
- **About:** displays product version information and license information, and enables license import.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

The following functions may be displayed, depending on the configuration of the system:

- **Open eToken SSO**: launches the *eToken Single Sign-On* application. This function is available only if *eToken SSO* is installed.
- **SAM Agent:** launches the *SAM Desktop Agent* application. For more information, see the SafeNet Authentication Manager User's Guide.
- **Delete Token Content:** removes the deletable data from the selected token.
- **Generate OTP:** generates an OTP on the selected *SafeNet eToken Virtual* token. This function is available only if the selected SafeNet eToken Virtual is configured to support this function.
- **Synchronize Password:** Synchronizes your Token Password with your domain password. Use this feature only if requested by your administrator.

SafeNet Authentication Client Icon Functions (BSec-Compatible Mode)

The following functions can be accessed quickly from the tray menu:

- **Change PIN:** opens the *Change PIN* window for the selected token.
- **Disable Event Notifications:** disables the *Event Notification* function.
- **Enrollment:** opens the *Enrollment* feature in the SafeNet Token Manager utility application.

- **Enrollment Update:** opens the *Enrollment Update* feature in the SafeNet Token Manager utility application.
- **Select Token:** allows you to select one of the connected tokens to be the active token. This function is available only when more than one token is connected.
- **About:** displays product information.
- **Exit:** closes SafeNet Authentication Client and the tray icon.

SafeNet Authentication Client Tools

Administrators use SafeNet Authentication Client Tools to set token policies. Users use SafeNet Authentication Client Tools to perform basic token management functions, such as changing passwords and viewing certificates on a connected token. In addition, SafeNet Authentication Client Tools provides users and administrators with a quick and easy way to transfer digital certificates and keys between a computer and a token.

SafeNet Authentication Client Tools includes an initialization feature allowing administrators to initialize tokens according to specific organizational requirements or security modes, and a password quality feature which sets parameters to calculate a Token Password quality rating.

> **CAUTION**
>
> Do not disconnect a token from the USB port, or a smart card from the reader, during an operation. This may cause corruption of the data on the token or smart card.

SafeNet Authentication Client Tools includes two viewing options:

- **Simple view:** to perform common tasks.

  See *Opening the Simple View* on page 20.

- **Advanced view:** for extensive control over SafeNet Authentication Client and your connected tokens.

  See *Opening the Advanced View* on page 25.

Each view displays two panes:

- The left pane indicates which token (Simple view) or which object (Advanced view) is to be managed.
- The right pane enables the user to perform specific actions to the selected token or object.

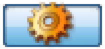
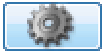
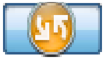
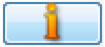
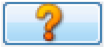
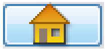
A toolbar at the top of the window enables certain actions to be initiated in both views.

NOTE

If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different than those displayed in this guide.

SafeNet Authentication Client Tools Toolbar

A toolbar is displayed at the top of SafeNet Authentication Client Tools, in both *Simple* and *Advanced* views. The toolbar contains the following icons:

Icon	Action
 	**Advanced View** – switches from the Simple to the Advanced view
	Simple View – switches from the Advanced to the Simple view
	**Refresh** – refreshes the data for all connected tokens
	**About** – displays product version information and license information, and enables license import
	**Help** – opens the Help feature
	**Home** – opens the company website

Opening the Simple View

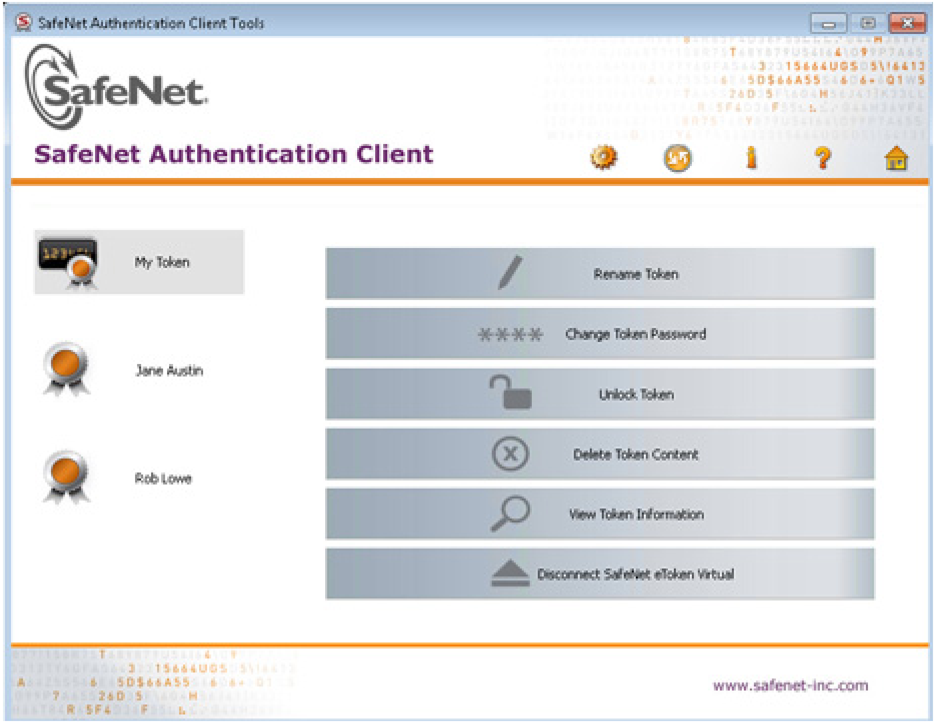
When SafeNet Authentication Client Tools is opened, the *Simple* view is displayed.

To open SafeNet Authentication Client Tools:

Do one of the following:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
- From the Windows taskbar, select **Start > Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

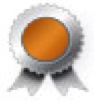
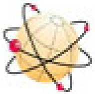
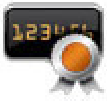
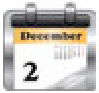
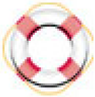
The *SafeNet Authentication Client Tools* window opens in the *Simple* view.

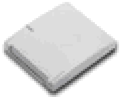
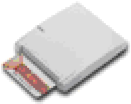
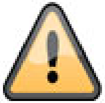
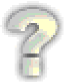


When tokens are connected, icons representing each connected token are displayed in the left pane. The selected token is marked by a shaded rectangle.

Token Icons

The icon displayed indicates the type of token that is connected.

Icon	Type
	eToken PRO (SafeNet eToken 5100) eToken NG Flash (SafeNet eToken 7100) SafeNet eToken Virtual iKey 4000 (SafeNet eToken 5000) iKey 2032 (SafeNet eToken 1000)
	eToken PRO Anywhere (SafeNet eToken 5200)
	eToken NG-OTP (SafeNet eToken 7000) SafeNet eToken Virtual, OTP enabled
	SafeNet eToken Virtual Temp
	SafeNet eToken Rescue

Icon (Cont.)	Type (Cont.)
	Smart card reader – no card connected
	Smart card reader – card connected: ♦ eToken PRO smart card (SafeNet eToken 4100) ♦ SafeNet smart card SC330 ♦ SafeNet SC400
	Token with corrupted data
	Unknown token

Simple View Functions

In the right pane, select an enabled button to perform the action described:

Function	Description
Rename Token	Sets the token name
Change Token Password	Changes the Token Password
Unlock Token	Unlocks the token and resets the Token Password
Delete Token Content	Removes deletable data from the token (enabled by default)
View Token Information	Provides detailed information about the token
Disconnect SafeNet eToken Virtual	Disconnects the SafeNet eToken Virtual or SafeNet eToken Rescue, with an option to also delete it

Opening the Advanced View

The SafeNet Authentication Client Tools *Advanced* view provides additional token management functions.

To open SafeNet Authentication Client Tools Advanced View:

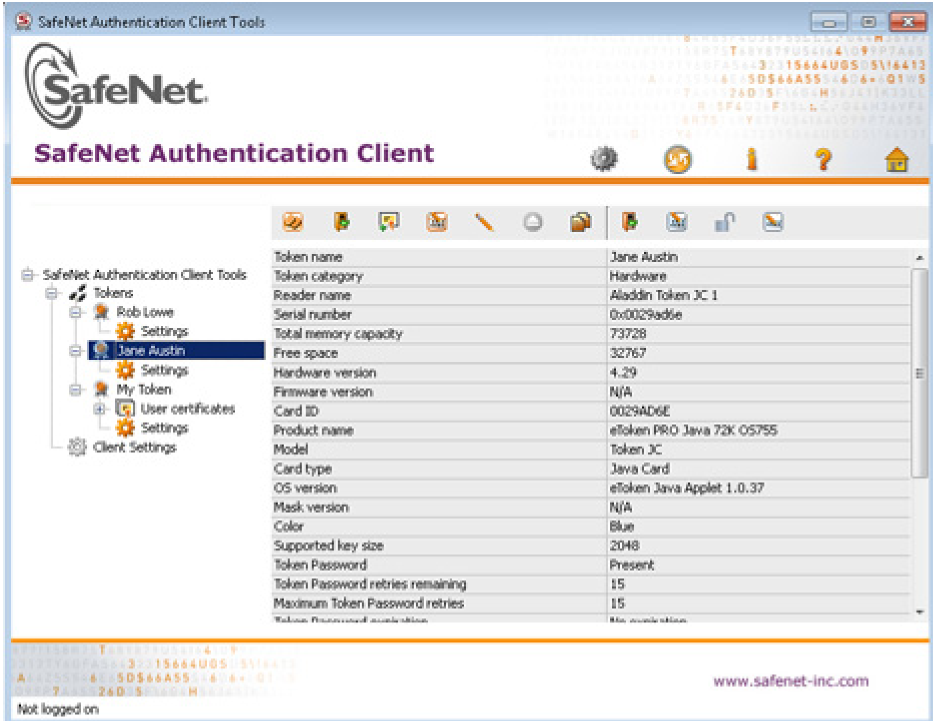
1 Do one of the following:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **Tools**.
- From the Windows taskbar, select **Start > Programs > SafeNet > SafeNet Authentication Client > SafeNet Authentication Client Tools.**

The *SafeNet Authentication Client Tools* window opens in the *Simple* view.

2 Click the **Advanced View** icon ⚙.

The *SafeNet Authentication Client Tools* window opens in the *Advanced* view.



Token name	Jane Austin
Token category	Hardware
Reader name	Aladdin Token JC 1
Serial number	0x0029ad6e
Total memory capacity	73728
Free space	32767
Hardware version	4.29
Firmware version	N/A
Card ID	0029AD6E
Product name	eToken PRO Java 72K OS755
Model	Token JC
Card type	Java Card
OS version	eToken Java Applet 1.0.37
Mask version	N/A
Color	Blue
Supported key size	2048
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration

The left pane provides a tree view of the different objects to be managed. The tree expands to show objects of the connected tokens.

Advanced View Functions

To access the advanced functions:

1. In the SafeNet Authentication Client Tools *Advanced View* window, expand the tree in the left pane to display the required object.

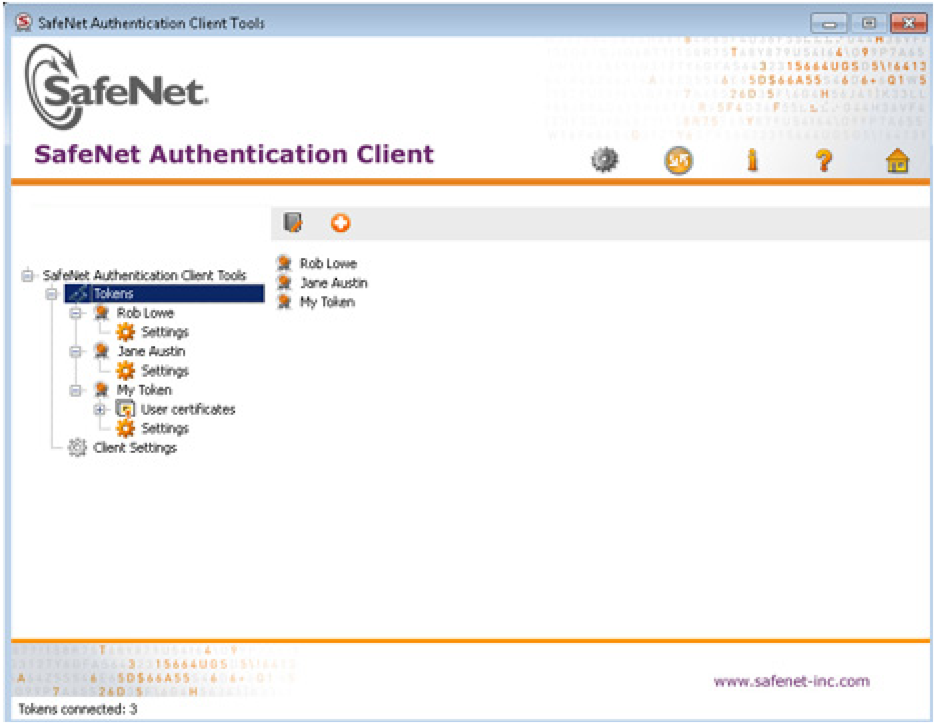
   The relevant functions are displayed in the right pane.

2. Do one of the following:

   - In the right pane, click the appropriate icon, or select the required tab.
   - In the left pane, right-click the object, and select the required function from the shortcut menu.

Tokens Node

When you select the *Tokens* node, the list of connected tokens is displayed in the right pane.



Tokens connected: 3

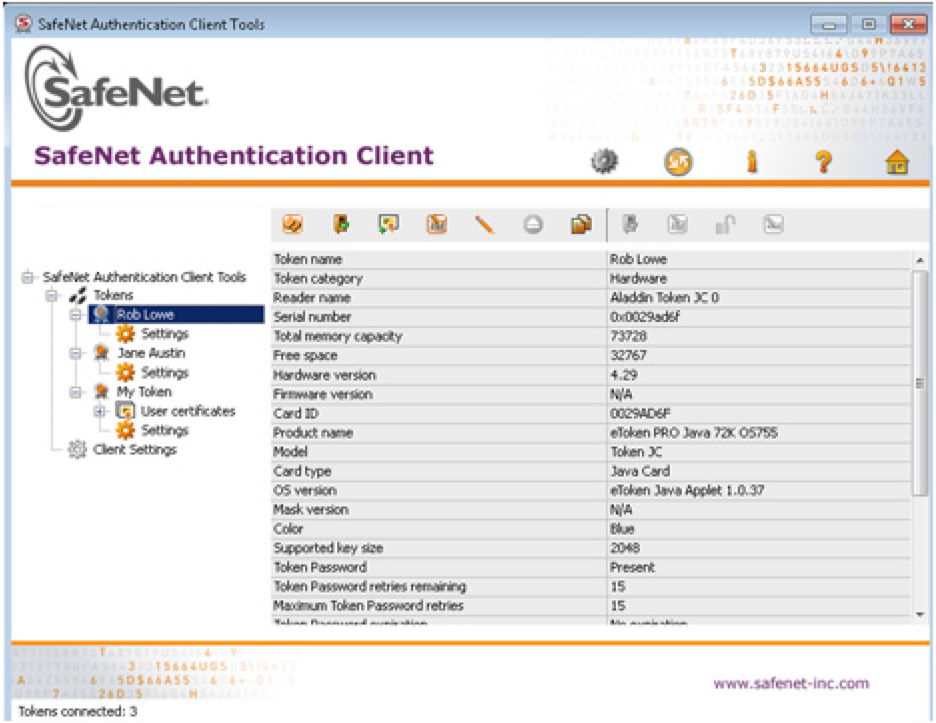
The following functions are available:

Function	Icon	Right-Click Menu Item
Reader Settings See *Reader Settings* on page 105.		Reader Settings
Connect SafeNet eToken Virtual See *Connecting a SafeNet eToken Virtual* on page 130.		Connect SafeNet eToken Virtual

Selected Token Node

The token names are displayed in the left pane. When you select a token name, the following occurs:

- information about the token is displayed in the right pane
- the name of the token reader is displayed in the tool-tip



Token name	Rob Lowe
Token category	Hardware
Reader name	Aladdin Token JC 0
Serial number	0x0029ad6f
Total memory capacity	73728
Free space	32767
Hardware version	4.29
Firmware version	N/A
Card ID	0029AD6F
Product name	eToken PRO Java 72K OS755
Model	Token JC
Card type	Java Card
OS version	eToken Java Applet 1.0.37
Mask version	N/A
Color	Blue
Supported key size	2048
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration

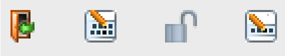
Tokens connected: 3

The following user functions are available:

User Function	Icon	Right-Click Menu Item
Initialize Token See *Token Initialization* on page 108.		Initialize
Log On to Token See *Logging On to the Token as a User* on page 51.		Log On
Import Certificate See *Importing a Certificate onto a Token* on page 71.		Import Certificate
Change Password See *Changing the Token Password* on page 56.		Change Password
Rename Token See *Renaming a Token* on page 53.	✎	Rename
Disconnect SafeNet eToken Virtual (SafeNet eToken Virtual or SafeNet eToken Rescue only) See *Disconnecting or Deleting a SafeNet eToken Virtual Product* on page 132.	⏏	Disconnect

User Function (Cont.)	Icon (Cont.)	Right-Click Menu Item (Cont.)
Copy to Clipboard See *Viewing and Copying Token Information* on page 48.	📋	None

Some administrator functions are available only if an Administrator Password has been set for the token. The administrator icons are located on the right of the window, enclosed within a border:



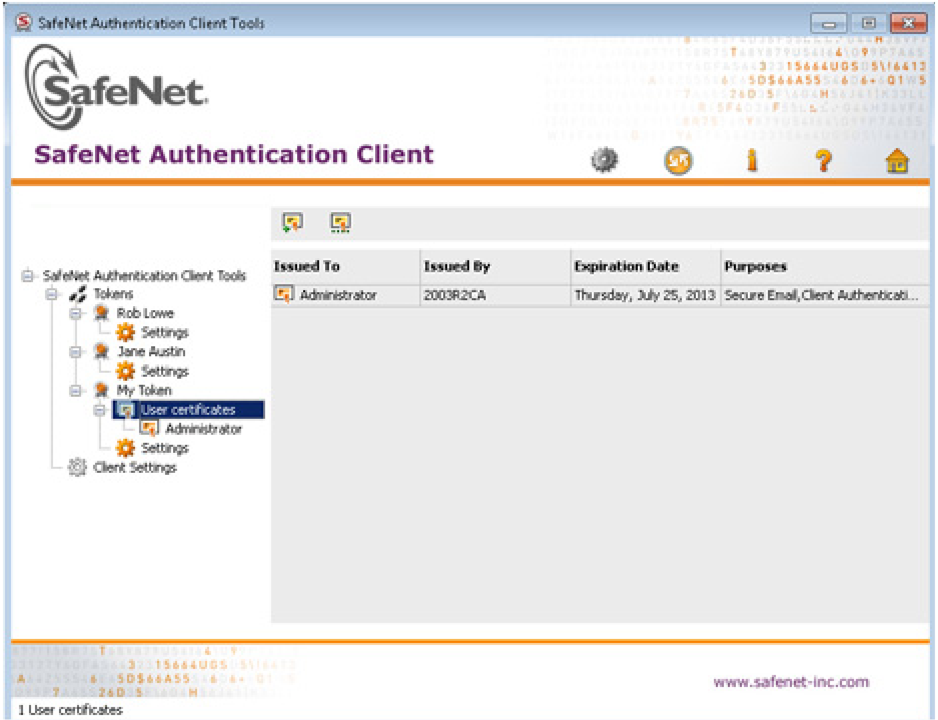
> **NOTE**
> When installing SAC in Bsec compatible mode, administrator password functions are not supported by iKey devices.

Certificates Nodes

If the selected token contains certificates, one or two appropriate nodes are displayed in the left pane under the token:

- User certificates
- CA certificates
- CC certificates

When you select one of these nodes, a list of the appropriate certificates on the token is displayed in the right pane.



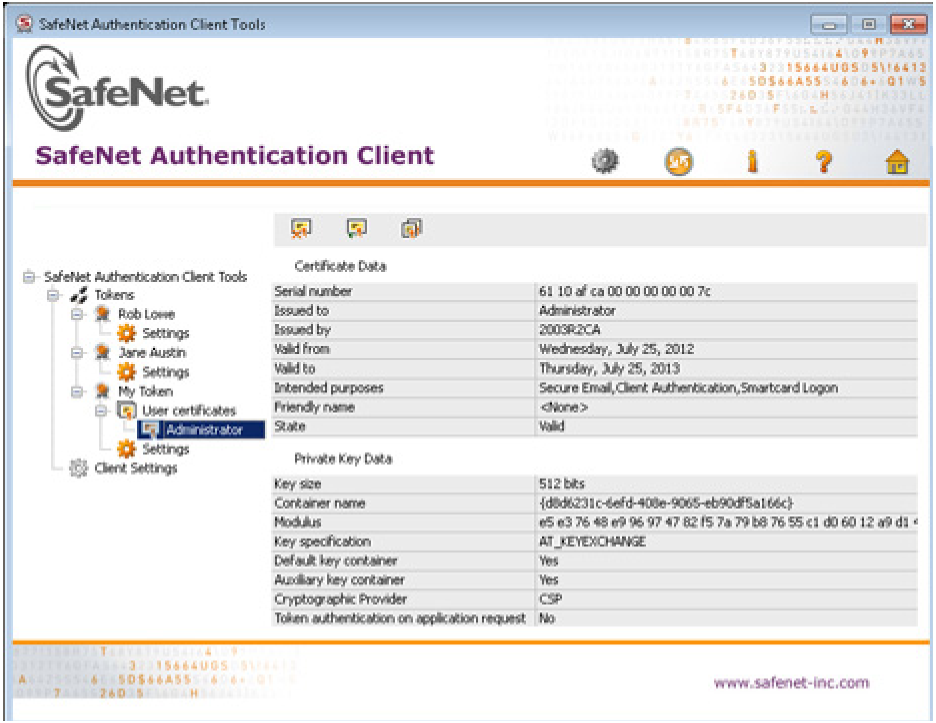
Issued To	Issued By	Expiration Date	Purposes
Administrator	2003R2CA	Thursday, July 25, 2013	Secure Email,Client Authenticati...

Depending on the certificate type, the following functions may be available:

User Function	Icon	Right-Click Menu Item
Import Certificate See *Importing a Certificate onto a Token* on page 71.		Import Certificate
Reset Default Certificate Selection See *Clearing a Default Certificate* on page 87.		Reset Default Certificate Selection

Selected Certificate Node

When you select a certificate under the *User certificates*, *CA certificates*, or *CC certificates* node, information about the certificate is displayed in the right pane.



Certificate Data

Serial number	61 10 af ca 00 00 00 00 00 7c
Issued to	Administrator
Issued by	2003R2CA
Valid from	Wednesday, July 25, 2012
Valid to	Thursday, July 25, 2013
Intended purposes	Secure Email,Client Authentication,Smartcard Logon
Friendly name	<None>
State	Valid

Private Key Data

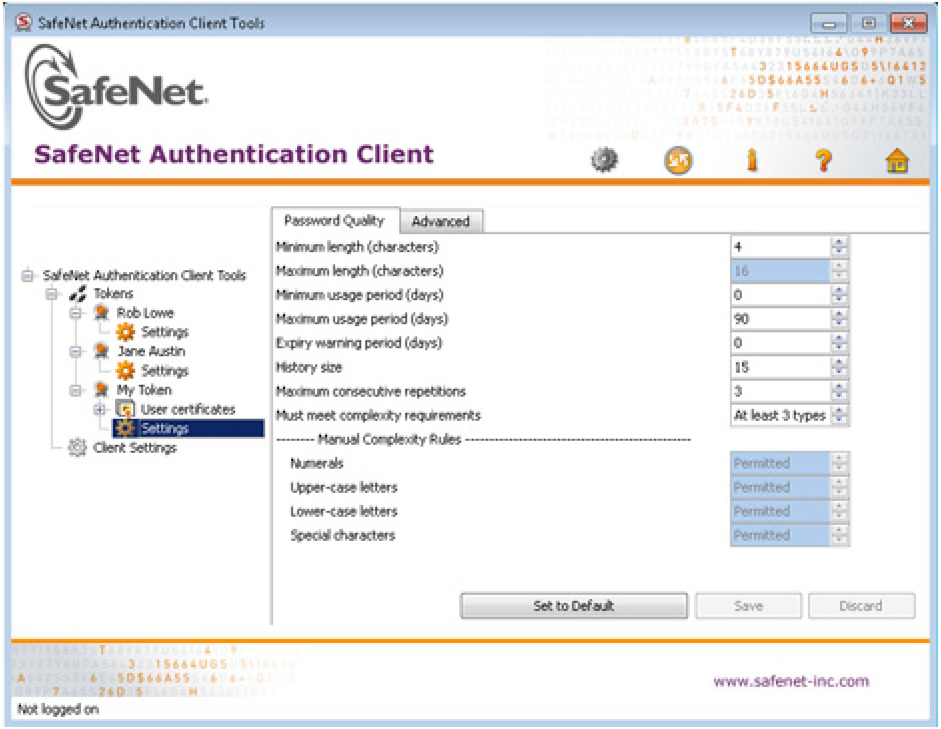
Key size	512 bits
Container name	{d8d6231c-6efd-408e-9065-eb90df5a166c}
Modulus	e5 e3 76 48 e9 96 97 47 82 f5 7a 79 b8 76 55 c1 d0 60 12 a9 d1
Key specification	AT_KEYEXCHANGE
Default key container	Yes
Auxiliary key container	Yes
Cryptographic Provider	CSP
Token authentication on application request	No

The following functions are available:

User Function	**Icon**	**Right-Click Menu Item**
Delete Certificate See *Deleting a Certificate* on page 89.		Delete Certificate
Export Certificate See *Exporting a Certificate from a Token* on page 77.		Export Certificate
Set as Default See *Setting a Certificate as Default or Auxiliary* on page 84.	n/a	Set as Default
Set as Auxiliary See *Setting a Certificate as Default or Auxiliary* on page 84.	n/a	Set as Auxiliary
Copy to Clipboard See *Viewing and Copying Token Information* on page 48.		None

Settings Node

Each connected token has a *Settings* node. Select it to open the *Settings* window in the right pane.



Minimum length (characters)	4
Maximum length (characters)	16
Minimum usage period (days)	0
Maximum usage period (days)	90
Expiry warning period (days)	0
History size	15
Maximum consecutive repetitions	3
Must meet complexity requirements	At least 3 types
-------- Manual Complexity Rules --------	
Numerals	Permitted
Upper-case letters	Permitted
Lower-case letters	Permitted
Special characters	Permitted

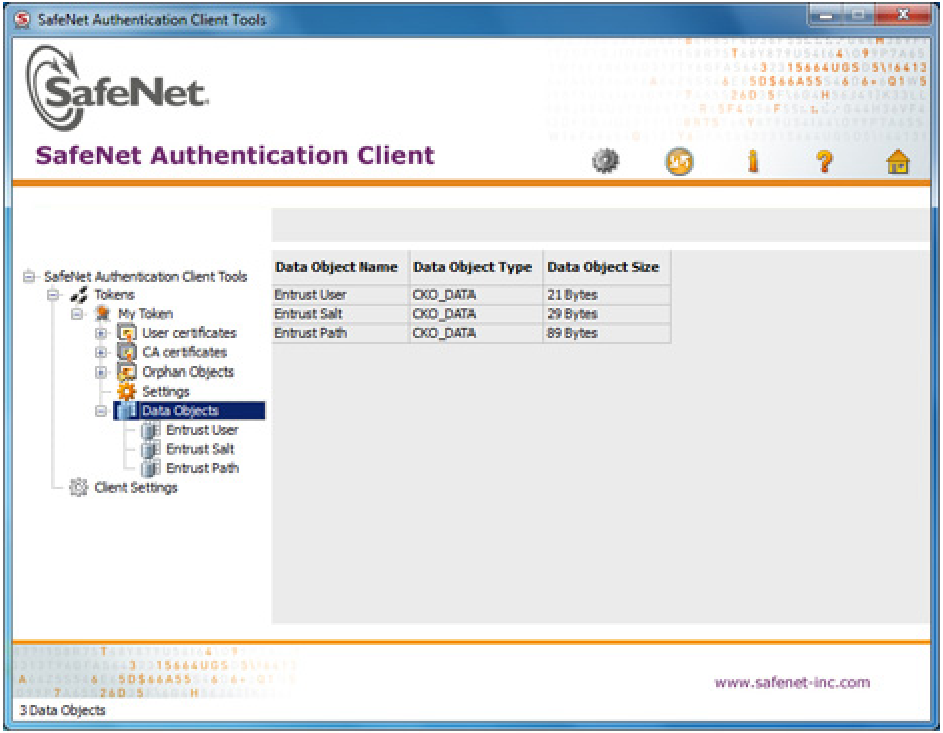
The *Settings* window contains two tabs:

- Password Quality (See *Setting Token Password Quality* on page 168.)
- Advanced (See *Setting Private Data Caching Mode* on page 173 and *Setting RSA Key Secondary Authentication* on page 176.)

NOTE
The *Advanced* tab is not used for iKey devices.

Data Objects Node

Tokens used together with Entrust applications contain PKCS#11 data objects.



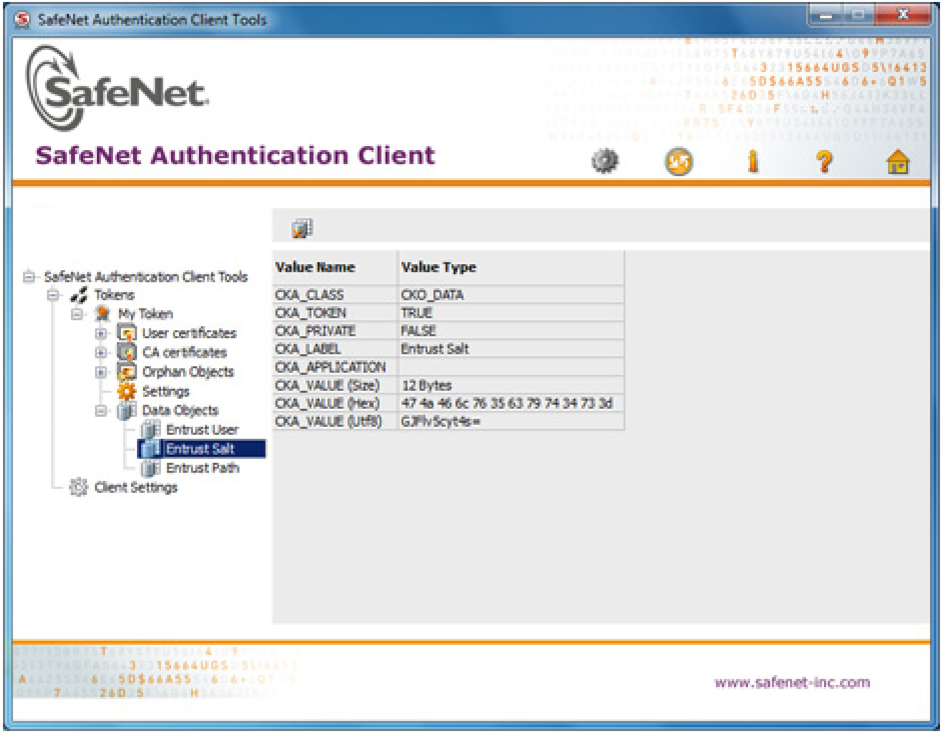
Data Object Name	Data Object Type	Data Object Size
Entrust User	CKO_DATA	21 Bytes
Entrust Salt	CKO_DATA	29 Bytes
Entrust Path	CKO_DATA	89 Bytes

To view the contents of a data object:

1 Expand the **Data Objects** node.

2 Select a data object.

The contents of the data object (**Name, Type** and **Size**) are displayed in the right pane.



Value Name	Value Type
CKA_CLASS	CKO_DATA
CKA_TOKEN	TRUE
CKA_PRIVATE	FALSE
CKA_LABEL	Entrust Salt
CKA_APPLICATION	
CKA_VALUE (Size)	12 Bytes
CKA_VALUE (Hex)	47 4a 46 6c 76 35 63 79 74 34 73 3d
CKA_VALUE (Utf8)	GJFlv5cyt4s=

To delete a data object:

1. Select the value to be deleted.
2. Click the **Delete Data Object** icon .

Client Settings Node

Select the *Client Settings* node to open the *Client Settings* window in the right pane.

The changes you make to the *Client Settings* window will affect all tokens that will be initialized after the changes have been saved.

Like the *Settings* window, the *Client Settings* window contains two tabs:

- Password Quality
- Advanced

See *Client Settings* on page 150.

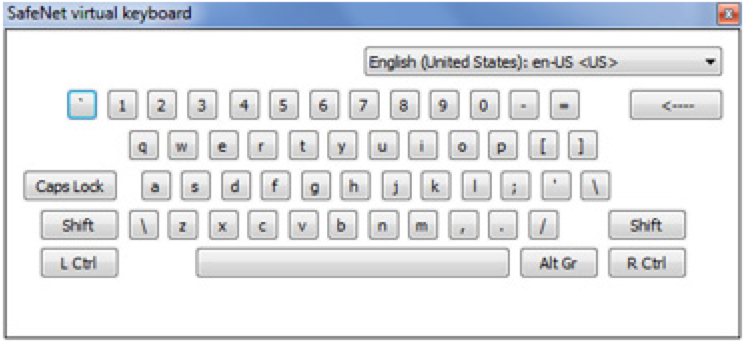
Using the Virtual Keyboard

The Virtual Keyboard provides you with an additional layer of security by enabling you to enter passwords without using the physical keyboard, providing protection against kernel level key loggers. The Virtual Keyboard is activated via the ADM Policy.

If your installation has been configured to use the Virtual Keyboard, it will be used in the following windows:

- Log on
- Change Password

The Virtual Keyboard icon appears in the password text box. Simply click inside the text box and the Virtual Keyboard opens.



SafeNet virtual keyboard

English (United States): en-US <US>

NOTE

When the Virtual Keyboard is active, you may use only the Virtual Keyboard and not your physical keyboard.

3 Token Management

SafeNet Authentication Client Tools and the SafeNet Authentication Client tray menu enable you to control the use of your tokens.

NOTE
If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different than those displayed in this guide.

In this chapter:

- Deleting Token Content
- Importing a Certificate onto a Token
- Exporting a Certificate from a Token
- Viewing Supported Cryptographic Providers
- Setting a Certificate as KSP or CSP
- Setting a Certificate as Default or Auxiliary
- Clearing a Default Certificate
- Deleting a Certificate
- Logging On to the Token as an Administrator
- Changing the Administrator Password
- Unlocking a Token by an Administrator
- Synchronizing Passwords
- Working with IdenTrust
- Reader Settings

Selecting the Active Token

If more than one token is connected, you can select which token to work with.

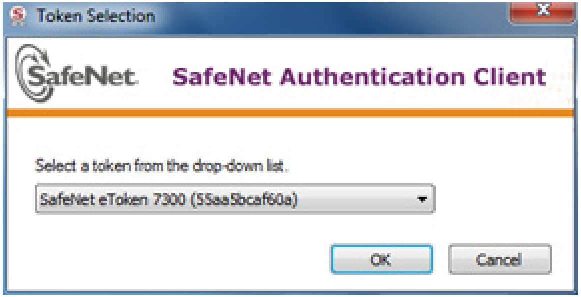
To use the tray menu to set a token as the active token:

1 Right-click the SafeNet Authentication Client tray icon.

The SafeNet Authentication Client tray menu opens.

2 Click **Select Token.**

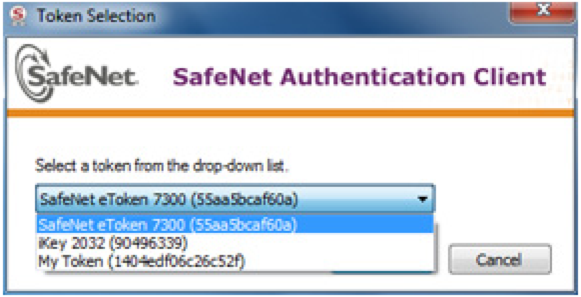
The *Token Selection* window opens.



Select a token from the drop-down list.

SafeNet eToken 7300 (55aa5bcaf60a)

3 Click the arrow to open the list of connected tokens**.**



Select a token from the drop-down list.

SafeNet eToken 7300 (55aa5bcaf60a)

SafeNet eToken 7300 (55aa5bcaf60a)
iKey 2032 (90496339)
My Token (1404edf06c26c52f)

4 Select the required token from the drop-down list.

5 Click **OK**.

To use SafeNet Authentication Client Tools to set a token as the active token:

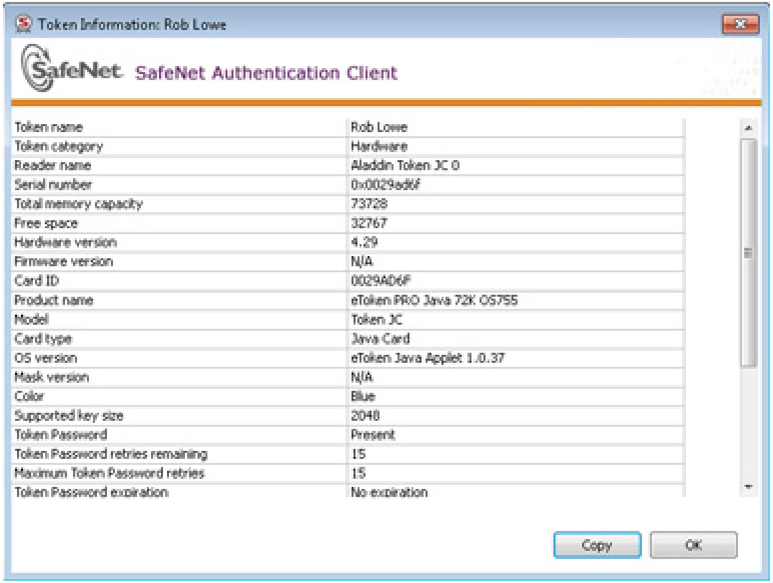
1 Open SafeNet Authentication Client Tools.
See Opening the Simple View on page 20 or See Opening the Advanced View on page 25.

2 In the left pane, select the required token.

Viewing and Copying Token Information

To view and copy token information:

1. To use the Simple View to view token information, do the following:
   - a. Open SafeNet Authentication Client Tools *Simple View.*
     See Opening the Simple View on page 20.
   - b. In the left pane, select the required token.
   - c. In the right pane, select **View Token Information**.
   - d. Continue with step 3.
2. To use the Advanced View to view token information, do the following:
   - a. Open SafeNet Authentication Client Tools *Advanced View.*
     See Opening the Advanced View on page 25.
   - b. In the left pane, select the node of the required token.
   - c. Continue with step 3.
3. The *Token Information* is displayed.



Token name	Rob Lowe
Token category	Hardware
Reader name	Aladdin Token JC 0
Serial number	0x0029ad6f
Total memory capacity	73728
Free space	32767
Hardware version	4.29
Firmware version	N/A
Card ID	0029AD6F
Product name	eToken PRO Java 72K OS755
Model	Token JC
Card type	Java Card
OS version	eToken Java Applet 1.0.37
Mask version	N/A
Color	Blue
Supported key size	2048
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration

The information displayed may vary according to the type of token.

4 To copy the token information to the clipboard, do one of the following:

- In the *Token Information* window, click **Copy**.
- In Advanced view, click the **Copy to Clipboard** icon:

5 To paste the copied token information, click the cursor in the target application, and paste the information.

6 Click **OK**.

Logging On to the Token as a User

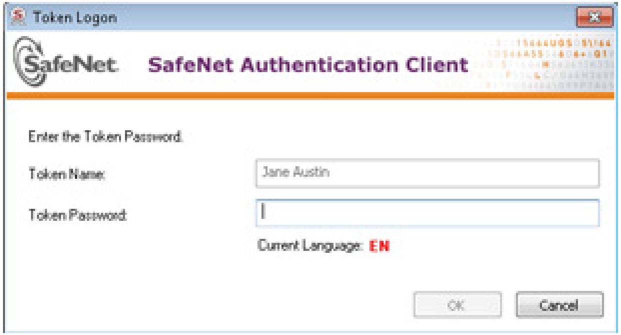
You must log on to the token before you can use or change its token content.

To log on as a user:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Log On to Token** icon:
   - In the left pane, right-click the node of the required token, and select **Log On** from the shortcut menu.

> **NOTE**
> If the **Log Off to Token** icon or the Log Off option is displayed, you are already logged on to the token

3. The *Token Logon* window opens.



Enter the Token Password.

Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK.**

You are logged on to the token.

Renaming a Token

The token name does not affect the token contents. It is used solely to identify the token.

> **TIP**
>
> If you have more than one token, we recommend assigning each one a unique token name.

To rename a token:

1. To use the Simple View to rename a token, do the following:
   a. Open SafeNet Authentication Client Tools *Simple View.*
      See Opening the Simple View on page 20.
   b. In the left pane, select the required token.
   c. In the right pane, select **Rename Token**.
   d. Continue with step 3.
2. To use the Advanced View to rename a token, do the following:

a Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

b Do one of the following:

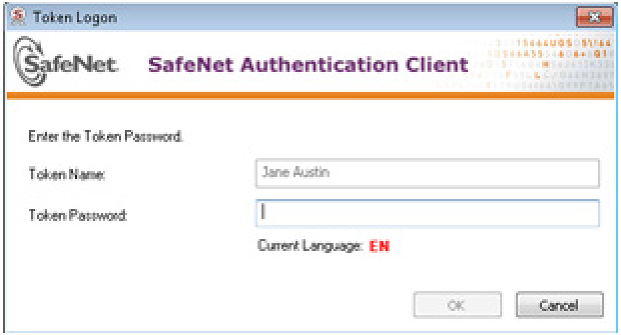
- In the left pane, select the node of the required token.
  In the right pane, click the **Rename Token** icon:

  ✎

- In the left pane, right-click the node of the required token, and select **Rename Token** from the shortcut menu.

c Continue with step 3.

3 The *Token Logon* window opens.



Enter the Token Password.

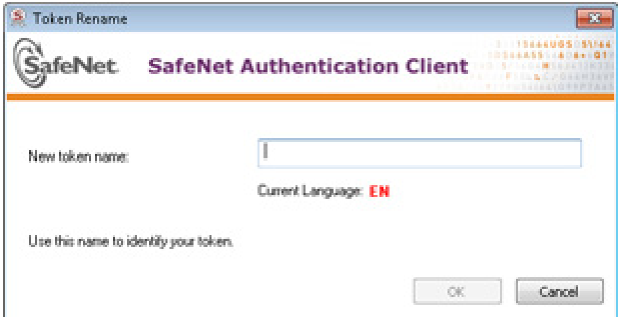
Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK**.

The *Rename Token* window opens.



New token name:

Current Language: EN

Use this name to identify your token.

5 Enter the new name in the *New token name* field, and click **OK**.

The new token name is displayed in the *SafeNet Authentication Client Tools* window.

Changing the Token Password

TIP

The term *Token Password* may be replaced by another term (for example, *Token PIN*), depending on your SafeNet Authentication Client configuration.

SafeNet eTokens are supplied with an initial default Token Password: **1234567890**.

To ensure strong, two-factor security, it is important for the user to change the initial Token Password to a private password as soon as the new token is received.

When a Token Password has been changed, the new password is used for all token applications involving the token. It is the user’s responsibility to remember the Token Password. Without it, the user cannot use the token.

The token’s *Password Quality* feature enables the administrator to set certain complexity and usage requirements for the password.

NOTE

The Token Password is an important security measure in safeguarding your company’s private information. The best passwords are at least eight characters long, and include upper- and lower-case letters, punctuation marks, and numbers appearing in a random order. We recommend against using passwords that can be easily discovered, such as names or birth dates of family members.

To change the Token Password:

1 To use the Simple View to change the Token Password, do the following:

   a Open SafeNet Authentication Client Tools *Simple View.*
   See Opening the Simple View on page 20.

   b In the left pane, select the required token.

   c In the right pane, select **Change Token Password**.

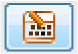
   d Continue with step 4.

2 To use the Advanced View to change the Token Password, do the following:

   a Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.

   b Do one of the following:

   - In the left pane, select the node of the required token.
     In the right pane, click the **Change Token Password** icon:

   - In the left pane, right-click the node of the required token, and select **Change Token Password** from the shortcut menu.

   c Continue with step 4.

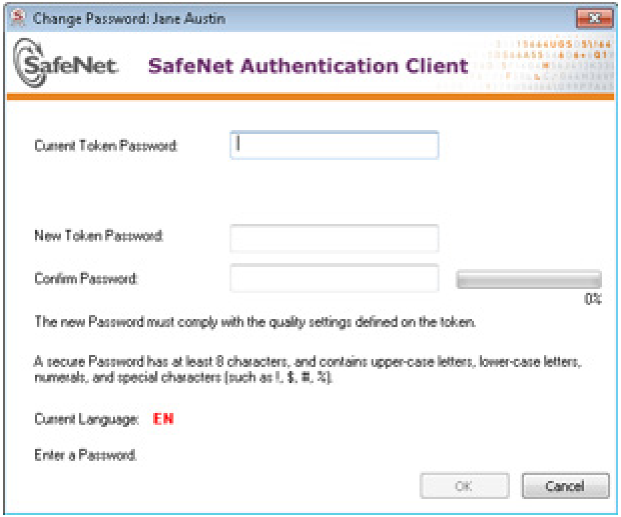
3 To use the tray menu to change the Token Password, do the following:

a Right-click the SafeNet Authentication Client tray icon.

b Select **Change Token Password**.

c Continue with step 4.

4 The *Change Password* window opens.



The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %)

Current Language: EN

Enter a Password.

5 Enter the current Token Password in the *Current Token Password* field.

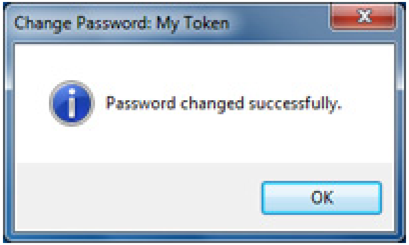
NOTE
If an incorrect password is entered more than a pre-defined number of times, the token will be locked.

6 Enter a new Token Password in the *New Token Password* and *Confirm Password* fields.

NOTE
As you type a new password, the password quality indicator on the right displays a percentage score of how well the new password matches the password quality requirements.

7 Click **OK**.

A message confirms that the Token Password was changed successfully.



Password changed successfully.

8 Click **OK**.

Unlocking a Token by the Challenge-Response Method

If an incorrect Token Password is entered more than a pre-defined number of times, the token will be locked. Tokens, including SafeNet eToken Virtual tokens, can be unlocked if, and only if, an Administrator Password was set during initialization.

SafeNet eToken Rescue tokens cannot be unlocked.

CAUTION

The number of times that a token can be unlocked can be limited to a specific amount. If this number is exceeded and the token is locked, the token becomes unusable. If the token is a physical token, it must be initialized. If it is not a physical token, it must be replaced.

When the administrator has access to the user's token, the administrator can unlock the token using the *Set Token Password* feature. (See Unlocking a Token by an Administrator on page 96.)

Another way to unlock the token and set a new Token Password is to use the *Challenge – Response* authentication method. The user sends the administrator the *Challenge Code* supplied by SafeNet Authentication Client Tools, and then enters the *Response Code* provided by the administrator. The new Token Password set by the user replaces the previous password, and the token is unlocked.

This method requires a management system, such as SafeNet Authentication Manager, that can generate Response Codes.

NOTE

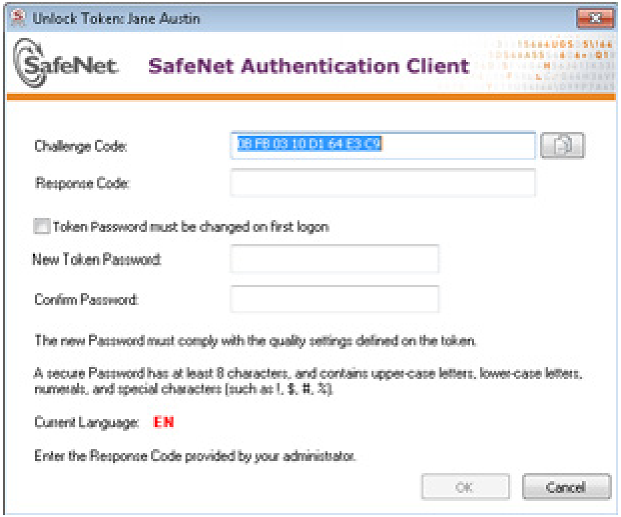
As of SAC 8.2 (standard mode), iKey devices are supported using the challenge response unlock method that is used for eTokens.

To unlock a token using the Challenge – Response method:

1. To use the Simple View to unlock a token, do the following:
   - a. Open SafeNet Authentication Client Tools *Simple View.*
     See Opening the Simple View on page 20.
   - b. In the left pane, select the required token.
   - c. In the right pane, select **Unlock Token**.
   - d. Continue with step 3.
2. To use the Advanced View to unlock a token, do the following:
   - a. Open SafeNet Authentication Client Tools *Advanced View.*
     See Opening the Advanced View on page 25.
   - b. Do one of the following:
     - In the left pane, select the node of the required token.
       In the right pane, click the **Unlock** icon:

       🔓

     - In the left pane, right-click the node of the required token, and select **Unlock** from the shortcut menu.
   - c. Continue with step 3.
3. *The Unlock Token* window opens, displaying a value in the *Challenge Code* field.



Challenge Code: 0B FB 03 10 D1 64 E3 C9

Response Code:

□ Token Password must be changed on first logon

New Token Password:

Confirm Password:

The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

Enter the Response Code provided by your administrator.

4 Contact your administrator, and provide the administrator with the *Challenge Code* value displayed.

NOTE

To copy the Challenge Code to the clipboard, click the Copy Challenge Code to clipboard icon:

CAUTION

After providing the Challenge Code to the administrator, **do not** undertake any activities that use the token until receiving the Response Code and completing the unlocking procedure.

If any other token activity occurs during this process, it will affect the context of the Challenge – Response process and invalidate the procedure.

5 The administrator provides you with the *Response Code* to be entered.

NOTE

Response Code creation depends on the back end application being used by the organization. Administrators should refer to the relevant documentation for information on how to generate the Response Code.

6 Enter a new Token Password in the *New Token Password* and *Confirm Password* fields.

7 If the new password is known to others and must be changed, select **Token Password must be changed on first logon**.

8 Click **OK**. A message confirms that the token was unlocked successfully.

9 Click **OK**.

Unlocking an iKey Token

An iKey token can be unlocked if it was configured with unblocking codes.

> **NOTE**
> This method of unlocking an iKey token is relevant for iKey tokens that were initialized using Bsec Utilities. Unlock is therefore applicable when using SAC tools, which was installed in Bsec Compatible mode.

To unlock an iKey token:

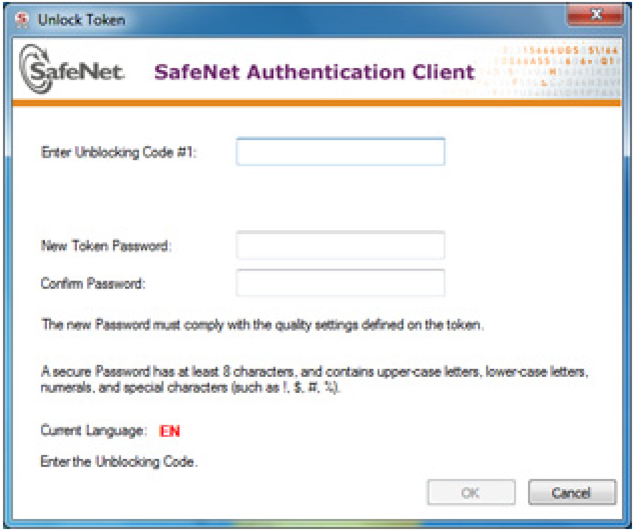
1. To use the Simple View to unlock an iKey token, do the following:
   - a Open SafeNet Authentication Client Tools *Simple View.*
     See Opening the Simple View on page 20.
   - b In the left pane, select the required token.
   - c In the right pane, select **Unlock Token**.
   - d Continue with step 3.
2. To use the Advanced View to unlock an iKey token, do the following:

a. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
b. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the **Unlock** icon:

     🔓

   - In the left pane, right-click the node of the required token, and select **Unlock** from the shortcut menu.
c. Continue with step 3.

3 *The Unlock Token* window opens.



Enter Unblocking Code #1:

New Token Password:

Confirm Password:

The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

Enter the Unblocking Code.

4 Enter one of the unblocking codes in the *Enter Unlocking Code* field.

NOTE

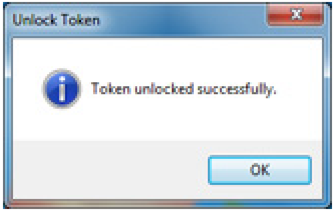
For iKey 4000:

- Up to six unblocking codes can be stored on each token and each unblocking code can be used only once.
- The unblocking codes can be used in any order.
- If only one unblocking code is configured, it can be re-used an unlimited number of times.

If more than one unblocking code is configured, each unblocking code can be used only once.

5 Enter a new password in the *New Token Password* and *Confirm Password* fields, and click **OK**.

A message confirms that the token was unlocked successfully.



Unlock Token

Token unlocked successfully.

6 Click **OK.**

Deleting Token Content

Objects on your token include data objects (profiles), keys, and CA or user certificates. Your system configuration determines which objects are deletable.

The *Delete Token Content* function deletes all deletable objects on your token. Non-deletable objects are not removed from the token. The function does not change settings on the token, such as password quality requirements.

The *Delete Token Content* function is less comprehensive than the *Initialize* function which restores a token to its initial state, removing all objects stored on the token since manufacture and resetting the Token Password. (See Token Initialization on page 108.)

To delete token content:

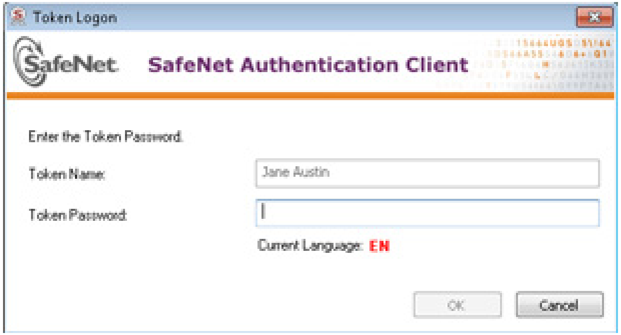
1. To use the Simple View to delete the token content, do the following:
   a. Open SafeNet Authentication Client Tools *Simple View.*
      See Opening the Simple View on page 20.
   b. In the left pane, select the required token.
   c. In the right pane, select **Delete Token Content**.
   d. Continue with step 3.
2. To use the tray menu to delete the token content, do the following:

a Right-click the SafeNet Authentication Client tray icon.

b Select **Delete Token Content**.

c Continue with step 3.

3 The *Token Logon* window opens.



Enter the Token Password.

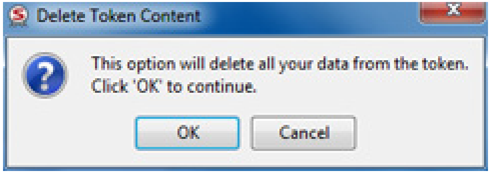
Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK**.

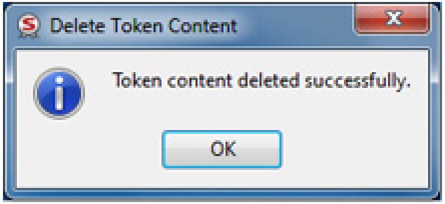
The *Delete Token Content* window opens, prompting you to confirm the delete action.



This option will delete all your data from the token.
Click 'OK' to continue.

5 To continue with the delete process, click **OK.**

The *Delete Token Content* window opens, confirming that the token content was deleted successfully.



Token content deleted successfully.

6 Click **OK** to finish.

Importing a Certificate onto a Token

The following certificate types are supported:

- .pfx
- .p12
- .cer

In the case of a PFX file, the private key and corresponding certificate will be imported to the token. If so configured, you will be asked if CA certificates should be imported to the token, and you will be asked to enter the password (if it exists) that protects the PFX file.

In the case of a CER file (which contains only X.509 certificates), the program checks if a private key exists on the token. If the private key is found, the certificate is stored with it. If no private key is found, then you are asked if you want to store the certificate as a CA certificate.

When downloading a certificate to the computer and then importing the certificate to the token, be sure to remove the certificate from the local store and then reconnect the token before using the certificate to sign and encrypt mail. This ensures that you are using the certificate and keys stored on the token and not on the computer.

> **NOTE**
> It is not possible to import a certificate onto a SafeNet eToken Rescue.

To import a certificate:

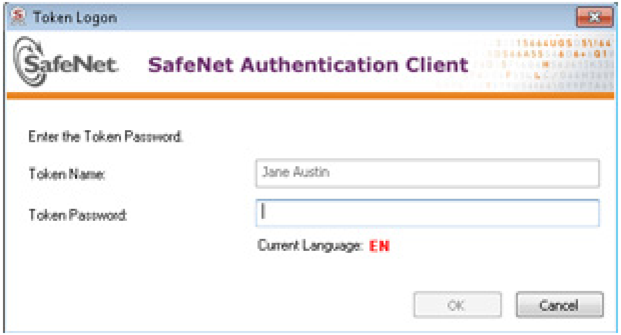
1 Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

2 Do one of the following:

- In the left pane, select the node of the required token.
In the right pane, click the **Import Certificate** icon.

- In the left pane, right-click the node of the required token, and select **Import Certificate** from the shortcut menu.

3 The *Token Logon* window opens.



Enter the Token Password.

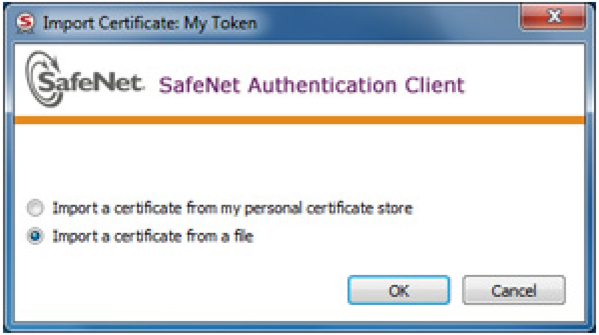
Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK**.

The *Import Certificate* window opens.



Import Certificate: My Token

SafeNet Authentication Client

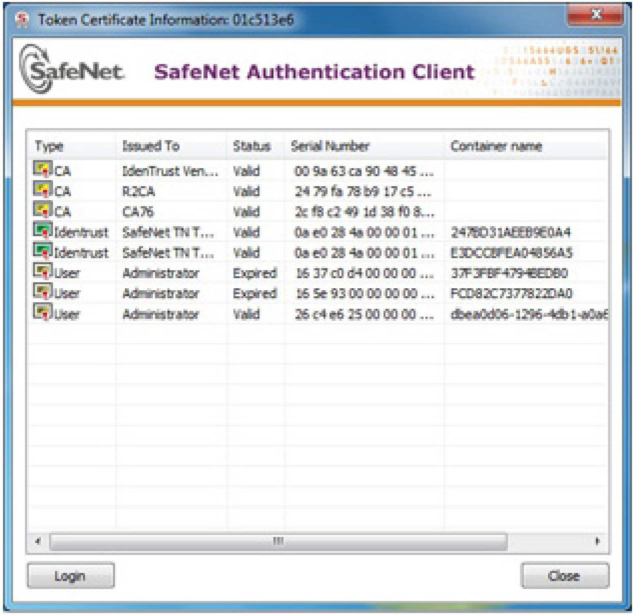
○ Import a certificate from my personal certificate store

● Import a certificate from a file

5 Select one of the following:

- ♦ Import a certificate from my personal certificate store
- ♦ Import a certificate from a file

6 If you select **Import a certificate from my personal certificate store**, a list of available certificates is displayed.

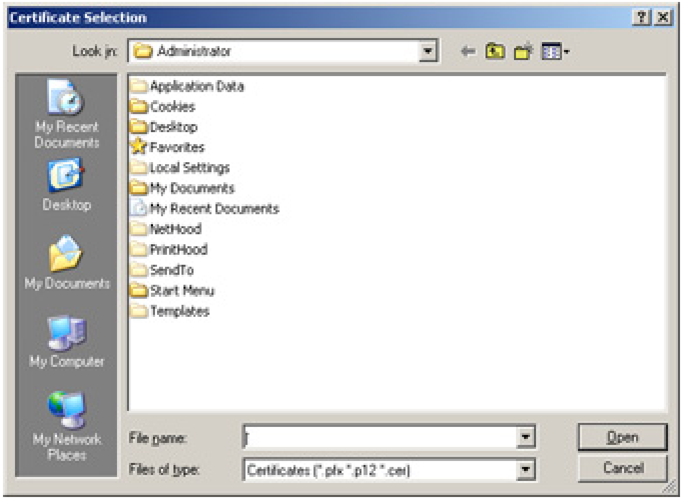

Token Certificate Information: 01c513e6
SafeNet
SafeNet Authentication Client

Type	Issued To	Status	Serial Number	Container name
CA	IdenTrust Ven...	Valid	00 9a 63 ca 90 48 45 ...	
CA	R2CA	Valid	24 79 fa 78 b9 17 c5 ...	
CA	CA76	Valid	2c f8 c2 49 1d 38 f0 8...	
Identrust	SafeNet TN T...	Valid	0a e0 28 4a 00 00 01 ...	247BD31AEEB9E0A4
Identrust	SafeNet TN T...	Valid	0a e0 28 4a 00 00 01 ...	E3DCCBFEA04856A5
User	Administrator	Expired	16 37 c0 d4 00 00 00 ...	37F3FBF47948ED80
User	Administrator	Expired	16 5e 93 00 00 00 00 ...	FCD82C7377822DA0
User	Administrator	Valid	26 c4 e6 25 00 00 00 ...	dbea0d06-1296-4db1-a0a6

Only certificates that can be imported on to the token are listed. These are:

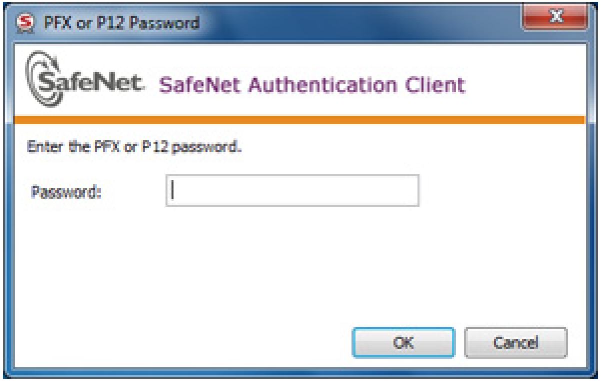
- Certificates with a private key already on the token
- Certificates that may be imported from the computer together with their private key

7 If you select **Import a certificate from a file**, the *Certificate Selection* window opens.



Select the certificate to import, and click **Open.**

8 If the certificate requires a password, the *Password* window opens.


PFX or P12 Password

SafeNet Authentication Client

Enter the PFX or P12 password.

Password:

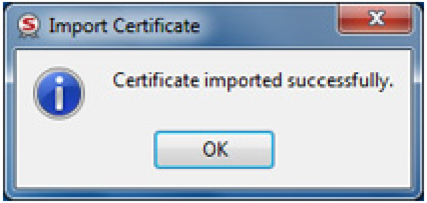
Enter the certificate password, and click **OK.**

9 If the certificate is a Common Criteria certificate, the *Import PIN* window opens.

Enter the token’s Import PIN defined during token initialization, and click **OK.**

The default value is **1234567890**.

10 All requested certificates are imported, and a message confirms that the import was successful**.**

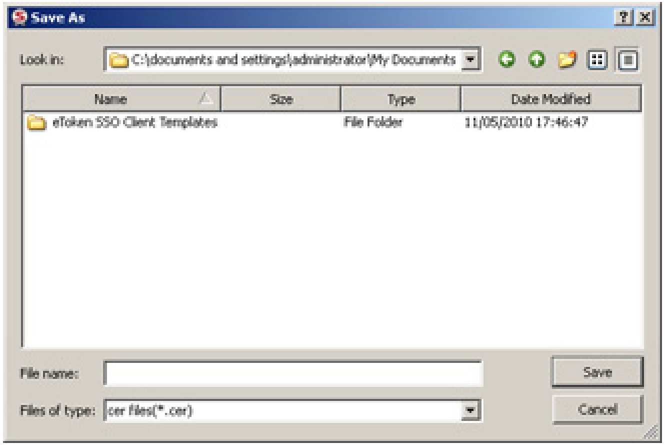

Import Certificate

Certificate imported successfully.

Exporting a Certificate from a Token

To export a certificate:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - Select the required certificate, and click the **Export Certificate** icon:
   - Right-click the required certificate, and select **Export Certificate** from the shortcut menu.
4. The *Save As* window opens.



Save As

Look in: C:\documents and settings\administrator\My Documents

Name	Size	Type	Date Modified
eToken SSO Client Templates		File Folder	11/05/2010 17:46:47

File name:

Files of type: cer files(*.cer)

5 Select the location to store the certificate, enter a file name, and click **OK**.

> **NOTE**
> The certificate file must be DER encoded or Base64 (not PKCS #7).

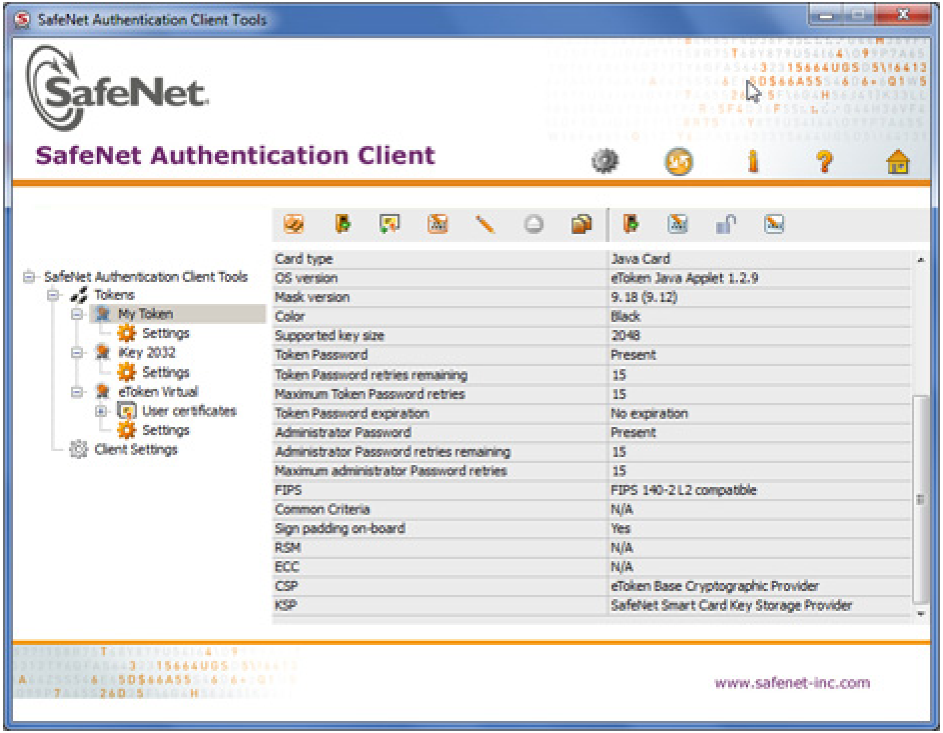
Viewing Supported Cryptographic Providers

When you select a token node in the SafeNet Authentication Client Tools *Advanced View*, the cryptographic providers supported by the token (KSP or CSP) are displayed.

To see which Cryptographic Providers are supported on the token:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select the node of the required token.

   Token data, including the supported cryptographic providers, is displayed in the right pane.



Card type	Java Card
OS version	eToken Java Applet 1.2.9
Mask version	9.18 (9.12)
Color	Black
Supported key size	2048
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration
Administrator Password	Present
Administrator Password retries remaining	15
Maximum administrator Password retries	15
FIPS	FIPS 140-2 L2 compatible
Common Criteria	N/A
Sign padding on-board	Yes
RSM	N/A
ECC	N/A
CSP	eToken Base Cryptographic Provider
KSP	SafeNet Smart Card Key Storage Provider

Setting a Certificate as KSP or CSP

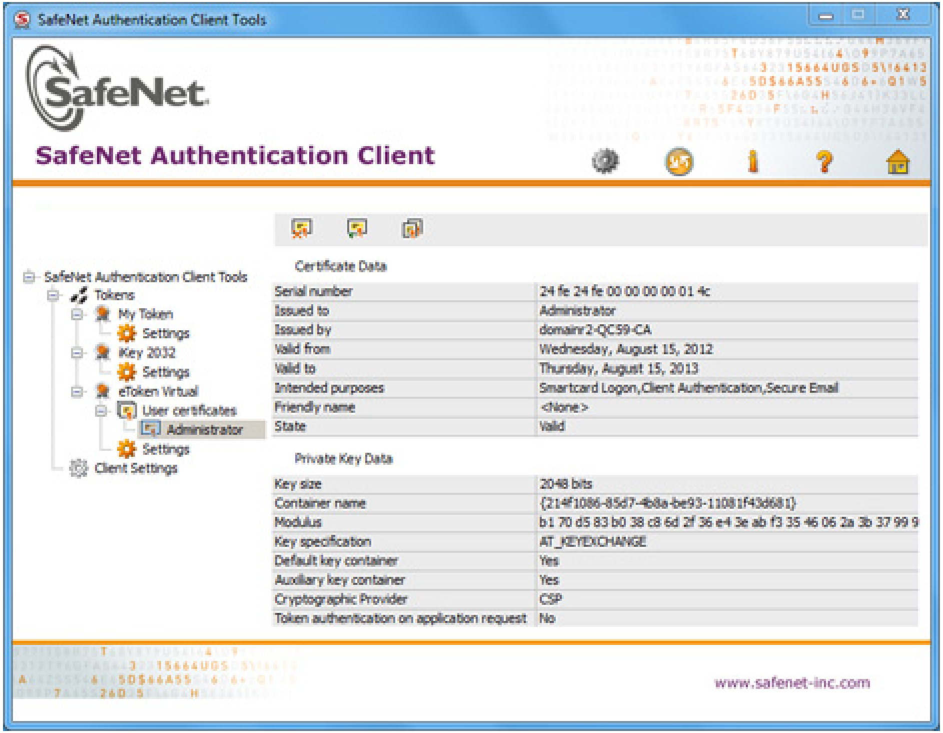
When you select a certificate node in the SafeNet Authentication Client Tools *Advanced View*, the cryptographic provider supported by the specific certificate is displayed under *Private Key Data*.

You can set a certificate type as Key Storage Provider (KSP) or Cryptographic Service Provider (CSP). This is typically required when you have a token enrolled with a legacy CSP that you want to convert to KSP, to enable support for the Suite B set of cryptographic algorithms (including SHA-2).

To set the certificate as KSP or CSP:

1 Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

2 In the left pane, expand the node of the required token.



Certificate Data

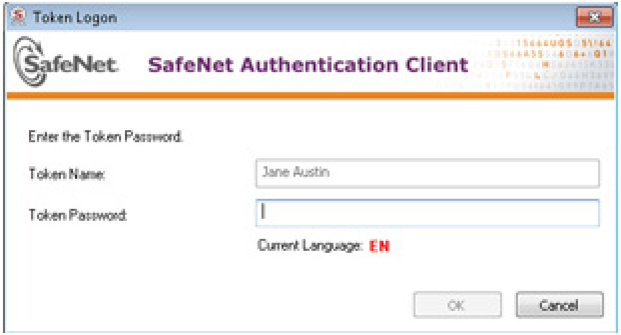
Serial number	24 fe 24 fe 00 00 00 00 01 4c
Issued to	Administrator
Issued by	domainr2-QC59-CA
Valid from	Wednesday, August 15, 2012
Valid to	Thursday, August 15, 2013
Intended purposes	Smartcard Logon,Client Authentication,Secure Email
Friendly name	<None>
State	Valid

Private Key Data

Key size	2048 bits
Container name	{214f1086-85d7-4b8a-be93-11081f43d681}
Modulus	b1 70 d5 83 b0 38 c8 6d 2f 36 e4 3e ab f3 35 46 06 2a 3b 37 99 9
Key specification	AT_KEYEXCHANGE
Default key container	Yes
Auxiliary key container	Yes
Cryptographic Provider	CSP
Token authentication on application request	No

3 Right-click the required certificate, and from the shortcut menu, select **Set as CSP** or **Set as KSP**.

4 The *Token Logon* window opens.



Token Logon

SafeNet Authentication Client

Enter the Token Password.

Token Name: Jane Austin

Token Password:

Current Language: EN

5 Enter the Token Password, and click **OK.**

The supported cryptographic provider is set.

Setting a Certificate as Default or Auxiliary

If there are multiple certificates on the token, you can determine which one is set as *Default* and which is set as *Auxiliary*.

Each option is enabled only if the action can be performed on that particular certificate or key.

The following table describes the use of these settings:

Setting	Description	Scenario
Default	Smart card logon uses the certificate defined as the *Default*. In most Microsoft applications, smart card logon is used.	Your token contains two certificates. One is for logon to domain A and the other for logon to domain B. Your previous logon was to domain A, which means that the certificate for logon to domain A is now the *Default*. If you now log on to domain B from another computer, the logon fails as it tries to use the domain A certificate. If you first set the domain B certificate as *Default*, the logon uses the correct certificate, and the logon succeeds.

Setting	Description (Cont.)	Scenario (Cont.)
Auxiliary	Some applications use Client Authentication and not smart card logon. Client Authentication provides access to fewer system resources than smart card logon. SafeNet Authentication Client enables a Client Authentication logon process for these applications, such as VPN. If more than one certificate on the token includes *Client Authentication* as an *Intended Purpose*, define which certificate to use by setting it as the *Auxiliary*.	Your token contains a certificate intended for VPN connection, but there is another certificate that also includes *Client Authentication* as its *Intended Purpose*. The certificate for the VPN connection must be set as *Auxiliary*, to ensure that it is used as the default for VPN logon.

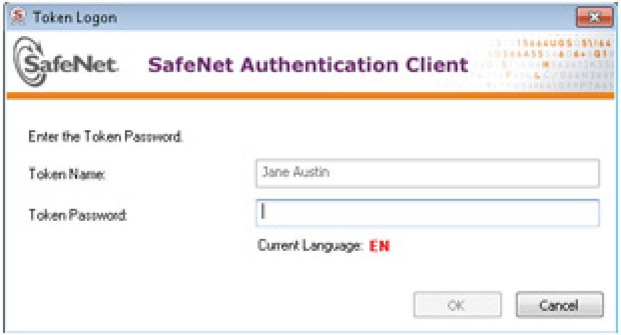
NOTE

iKey does not support Auxiliary certificates. It treats an Auxiliary certificate as a Default certificate.

To set a certificate as Default or Auxiliary:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token, and right-click the required certificate.
3. From the shortcut menu, select **Set as Default** or **Set as Auxiliary**.

   The *Token Logon* window opens.



Token Logon

SafeNet Authentication Client

Enter the Token Password.

Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK.**

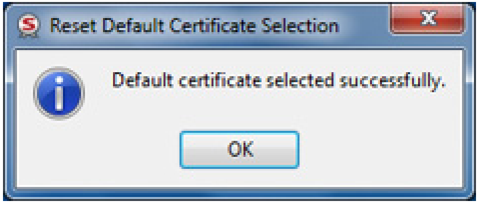
The certificate is set as *Default* or *Auxiliary*.

Clearing a Default Certificate

If you have set a certificate as Default, you can clear the setting and revert to using the previous Default certificate.

To clear a default certificate:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - In the left pane, select *User Certificates*.
     In the right pane, click the **Reset Default Certificate Selection** icon.
   - In the left pane, right-click *User Certificates*, and select **Reset Default Certificate Selection** from the shortcut menu.
4. The *Reset Default Certificate Selection* window opens, confirming that the Default certificate has been reset.



Reset Default Certificate Selection

Default certificate selected successfully.

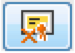
5 Click **OK**.

Deleting a Certificate

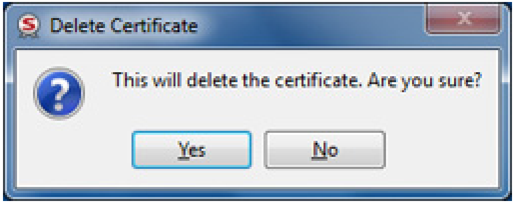
You can remove a certificate from a token.

To delete a certificate from a token:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token.
3. Do one of the following:
   - In the left pane, select the required certificate, and click the **Delete Certificate** icon.

   - In the left pane, right-click the required certificate, and select **Delete Certificate** from the shortcut menu.
4. The *Delete Certificate* window opens.

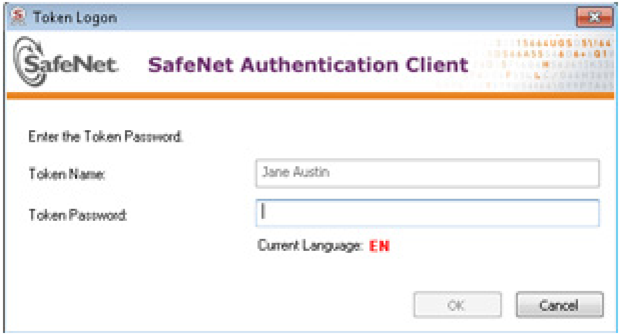


Delete Certificate

This will delete the certificate. Are you sure?

5 To delete the certificate, click **Yes.**

The *Token Logon* window opens.



Enter the Token Password.

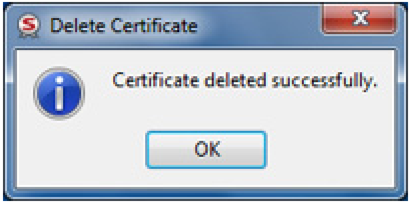
Token Name: Jane Austin

Token Password:

Current Language: EN

6 Enter the Token Password, and click **OK**.

The *Delete Certificate* window opens, confirming that the certificate was deleted successfully.



Certificate deleted successfully.

7 Click **OK.**

Logging On to the Token as an Administrator

If an Administrator Password was set on the token during token initialization, and the user forgets the Token Password, the Administrator Password can be used to unlock the token by setting a new Token Password. We recommend initializing all supported tokens with an Administrator Password.

> **NOTE**
> When installing SAC in Bsec compatible mode, administrator password functions are not supported by iKey devices.

An administrator has limited permissions on a token. No changes to any user information may be made by the administrator, nor may the user's security be affected. The administrator can change data stored on the token only by using the following functions:

- Changing the Administrator Password (not supported by iKey devices)
- Unlocking a Token by an Administrator
- Unlocking a Token by the Challenge-Response Method
- Setting Token Password Quality
- Setting Private Data Caching Mode
- Setting RSA Key Secondary Authentication

To log on to a token as an administrator:

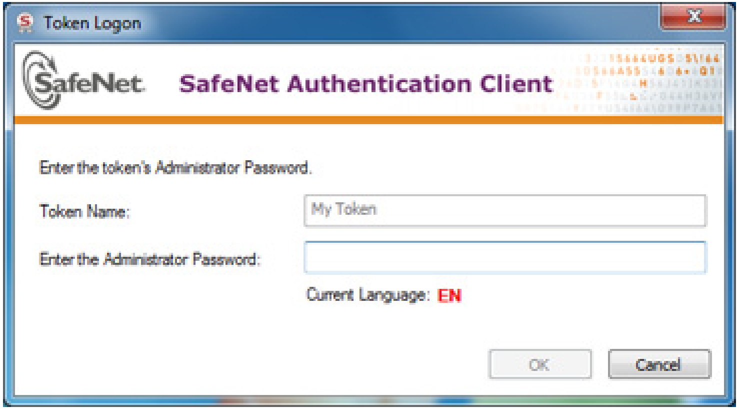
1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.

2 Do one of the following:

- In the left pane, select the node of the required token.
  In the right pane, click the **Log On as Administrator** icon:

- In the left pane, right-click the node of the required token, and select **Log On as Administrator** from the shortcut menu.

3 The *Token Logon* window opens.



Token Logon

SafeNet Authentication Client

Enter the token's Administrator Password.

Token Name: My Token

Enter the Administrator Password:

Current Language: EN

4 Enter the token’s Administrator Password, and click **OK**.

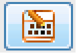
You are logged on as an administrator.

Changing the Administrator Password

If you are logged on to a token as an administrator, you can change the token’s Administrator Password.

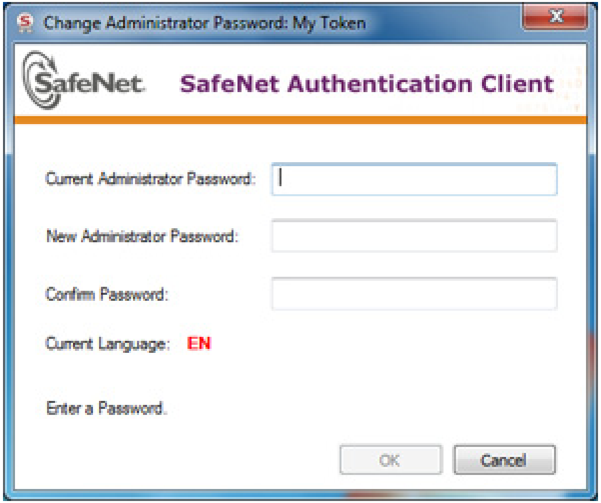
To change the Administrator Password:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. Do one of the following:
   - In the left pane, select the node of the required token.
     In the right pane, click the *Change Administrator Password* icon:

   - In the left pane, right-click the node of the required token, and select **Change Administrator Password** from the shortcut menu.

   The *Change Administrator Password* window opens.



Change Administrator Password: My Token

SafeNet Authentication Client

Current Administrator Password:

New Administrator Password:

Confirm Password:

Current Language: EN

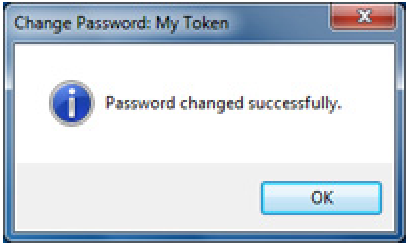
Enter a Password.

3 Enter the current Administrator Password in the *Current Administrator Password* field.

NOTE
If an incorrect Administrator Password is entered more than a pre-defined number of times, the token will be locked.

4 Enter the new password in the *New Administrator Password* and *Confirm Password* fields.

5 Click **OK**. A message confirms that the password was changed successfully.



Change Password: My Token

Password changed successfully.

6 Click **OK**.

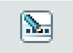
Unlocking a Token by an Administrator

If you are logged on to a token as an administrator, you can unlock the token by setting a new Token Password.

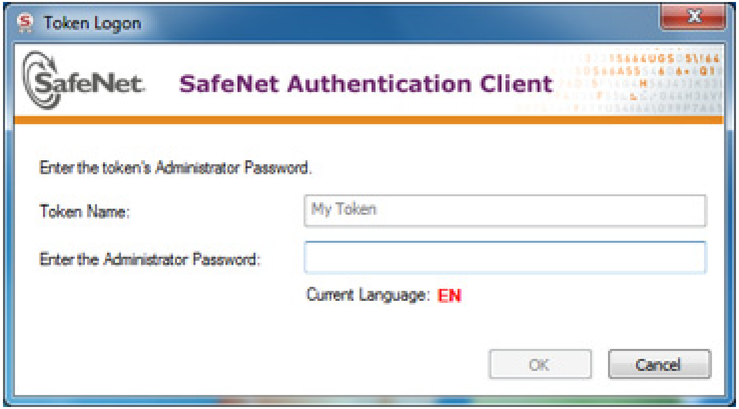
NOTE
The unlock feature may also be accessed by right-clicking the tray icon.

To unlock a token using *Set Token Password*:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select the appropriate token.
3. Click the **Set Token Password** icon:

   The *Token Logon* window opens.



Token Logon

SafeNet Authentication Client

Enter the token's Administrator Password.

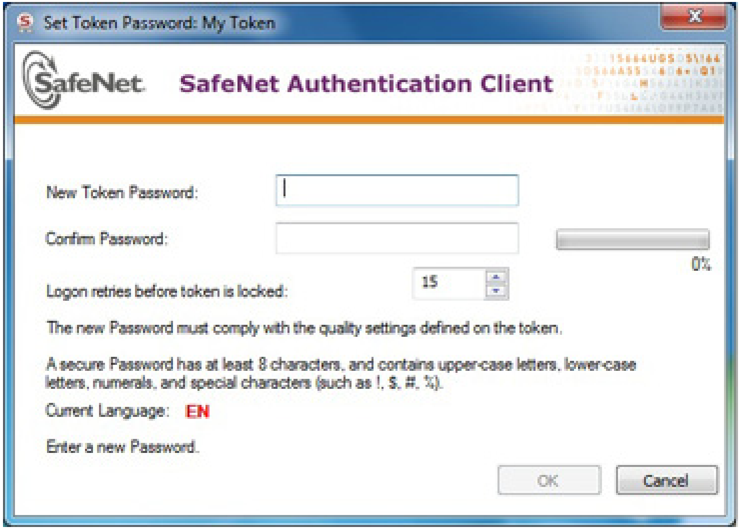
Token Name: My Token

Enter the Administrator Password:

Current Language: EN

4 Enter the Administrator Password, and click **OK**.

The *Set Token Password* window opens.



New Token Password:

Confirm Password: 0%

Logon retries before token is locked: 15

The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

Enter a new Password.

5 Enter a new Token Password in the *New Password* and *Confirm Password* fields.

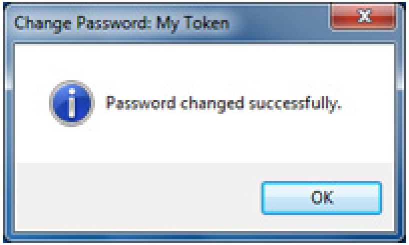
> **NOTE**
> The new Token Password must meet password quality settings as defined for the token.

6 Set the *Set maximum number of logon failures* field to the required number.

> **NOTE**
> The *Set maximum number of logon failures* feature is available only on CardOS tokens. Java card tokens are not supported.

7 Click **OK**.

A message confirms that the Token Password was changed successfully.



Password changed successfully.

8 Click **OK**.

The token is unlocked, and the user can now log on with the new Token Password.

Synchronizing Passwords

NOTE
Password synchronization is implemented only in specific installations of SafeNet Authentication Client, where it is required.

SafeNet Authentication Client supports synchronization between Token Passwords and domain logon passwords.

The synchronization process provides a single password that can be used for logging on to both the token and the Windows domain. The process ensures that the password complexity requirements as set for the token and SafeNet Authentication Client are met.

NOTE
The new password must meet the complexity requirements for the token and the domain. You must have access to the domain when changing the password.

To synchronize passwords:

1 Right-click the SafeNet Authentication Client tray icon.

The SafeNet Authentication Client tray menu opens.

2 Select **Synchronize Password.**

The *Synchronize Passwords* window opens.

3 Enter the current Token Password and the current domain password.

4 Enter the new Token Password, and confirm it.

5 Click **OK**.

You now have a single password for logging on to your token and Windows domain.

Every time you change your Token Password using SafeNet Authentication Client, the domain logon password will be synchronized with it.

Working with IdenTrust

IdenTrust supports two modes:

- **Token Password** - Token Password is used as an Identity PIN and is entered every time that an identity certificate is used. This is supported by all SafeNet eToken and iKey devices.
- **Identity PIN (Legacy)** - is used in legacy iKey 2032i devices. The Identity PIN is used in addition to the Token Password.

Using the Identity PIN (Legacy)

Changing the Identity PIN

To change the Identity PIN:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. Right-click the token, and select **Change Identity PIN**.
3. The *Change Identity PIN* window opens.
4. Enter the current PIN, and enter and confirm the new PIN.

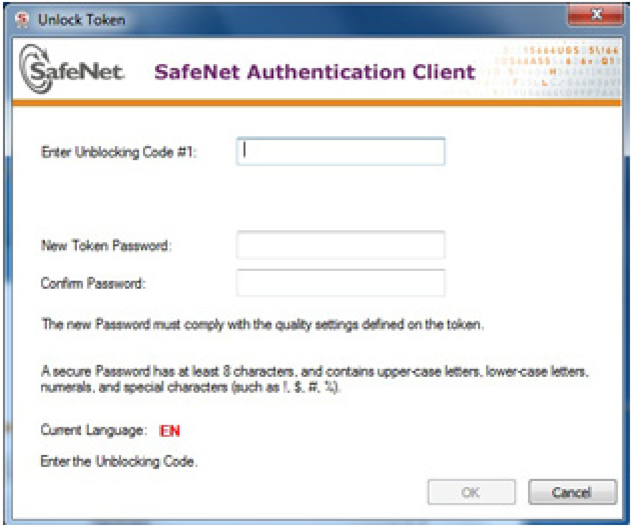
Unblocking the Identity PIN

If an incorrect Identity PIN is entered multiple times, the PIN becomes blocked. It must be unblocked to enable you to continue working with the token.

To unblock the Identity PIN:

1 Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

2 Right-click the token, and select **Unblock Identity**. The *Unblock Identrust PIN* window opens.



Enter Unblocking Code #1:

New Token Password:

Confirm Password:

The new Password must comply with the quality settings defined on the token.

A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

Enter the Unblocking Code.

3 Enter the unblocking code in the *Enter Unblocking Code* field.

4 Enter a new password in the *New Password* and *Confirm Password* fields, and click **OK**.

Reader Settings

During the installation of SafeNet Authentication Client, two virtual SafeNet eToken readers, two iKey readers, and one SafeNet eToken Virtual reader is installed.

The number of default SafeNet eToken readers or SafeNet eToken Virtual readers for a computer can be changed by a user with local administrator rights on that computer. The default number of iKey readers is set during installation and cannot be modified by the user after installation.

A token is connected to a reader when one of the following occurs:

- A token is inserted into a USB port
- A SafeNet eToken Virtual is connected
- A smartcard is inserted into a reader

To change the number of readers:

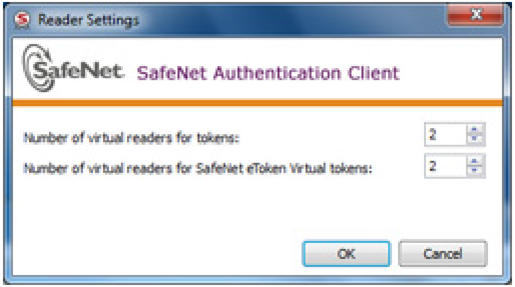
> **NOTE**
> This procedure applies only to SafeNet eToken readers and SafeNet eToken Virtual readers, and not to iKey readers.

1 Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

Do one of the following:

- In the left pane, select the **Tokens** node.
  In the right pane, click the **Reader Settings** icon:
  .
- In the left pane, right-click the **Tokens** node, and select **Reader Settings** from the shortcut menu.

2 The *Reader Settings* window opens.



Number of virtual readers for tokens: 2

Number of virtual readers for SafeNet eToken Virtual tokens: 2

3. Set the required number of virtual hardware or software readers in the appropriate field.

   The default number of available readers is:

   - Token readers: 2
   - SafeNet eToken Virtual readers: 2

4. Click **OK** to close the window.

   The number of available readers is changed.

5. Restart SafeNet Authentication Client Tools to make the changes effective.

4 Token Initialization

The token initialization process restores a token to its initial state.

NOTE
You cannot use SafeNet Authentication Client to initialize a SafeNet eToken Virtual product.

In this chapter:

Overview of Token Initialization

The token initialization process removes all objects stored on the token since manufacture, frees up memory, and resets the Token Password. Then the token is initialized with specific settings according to the organizational requirements or security modes.

Typically, initialization is carried out on a token when an employee leaves the company, enabling the token to be issued to another employee. It completely removes the employee's individual certificates and other personal data from the token, preparing it to be used by another employee.

The following data is initialized:

- Token name
- Token Password
- Administrator Password (optional) - not supported by iKey devices
- Maximum number of logon failures allowed
- Requirement to change the Token Password on the first logon
- Initialization key
- All user-generated data, such as certificates and profiles

Using customizable parameters, you may be able to select specific parameters that will apply to certain tokens. These parameters may be necessary if you wish to use a token for specific applications or if you require a specific Token Password or Administrator Password on multiple tokens in the organization.

Configuring Initialization Settings

> **NOTE**
> - Depending on the type of token being initialized, certain settings may not be enabled.
> - If a customized version of SafeNet Authentication Client is installed, the graphics you see may be different than those displayed in this guide.

To initialize a token:

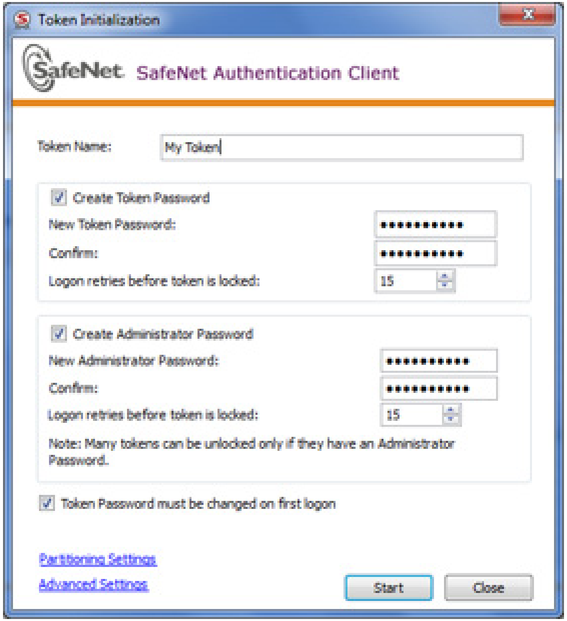
1. Open SafeNet Authentication Client Tools *Advanced View.*
   See <Emphasis>Opening the Advanced View on page 25.

2. Do one of the following:

   - In the left pane, select the node of the required token.
     In the right pane, click the **Initialize Token** icon:

   - In the left pane, right-click the node of the required token, and select **Initialize** from the shortcut menu.

   The *Token Initialization* window opens.



Token Initialization

SafeNet Authentication Client

Token Name: My Token

☑ Create Token Password

New Token Password: ***********

Confirm: ***********

Logon retries before token is locked: 15

☑ Create Administrator Password

New Administrator Password: ***********

Confirm: ***********

Logon retries before token is locked: 15

Note: Many tokens can be unlocked only if they have an Administrator Password.

☑ Token Password must be changed on first logon

3 Enter a name for the token in the *Token Name* field. If no name is entered, the default name, “My Token”, is applied.

The token name does not affect the token contents. It is used solely to identify the token.

4 Select **Create Token Password** to initialize the token with a Token Password.

If the token is initialized without a Token Password, it will not be usable for token applications.

5 Enter a new Token Password in the *New Token Password* and *Confirm* fields.

NOTE

- The default Token Password is 1234567890.
- If the token is initialized with the default Token Password, and password quality requirements are in effect, the user must select the Token Password must be changed on first logon option. Otherwise the initialization will fail, because the default password does not meet the default password quality requirements. If the Token Password must be changed on first logon option is selected, the initialization will succeed and the user will be prompted to create a new password when next logging on with the token. The user will be required to set a Token Password that meets the password quality requirements configured in the Settings window. See Setting Token Password Quality on page 168.

6 To initialize an Administrator Password, select **Set Administrator Password** and enter a password in the *New Administrator Password* and *Confirm* fields. The minimum password length is 4 characters.

NOTE

- Setting an Administrator Password enables certain functions to be performed on the token, such as setting a new Token Password to unlock a token.
- iKey tokens do not support Administrator Passwords.

7 In the *Logon retries before token is locked* field, enter a value between 1 and 15. This counter specifies the number of times the user or administrator can attempt to log on to the token with an incorrect password before the token is locked. The default setting for the maximum number of incorrect logon attempts is 15.

8 If required, select **Token Password must be changed on first logon**.

This is selected by default.

9 To configure the partitioning settings of SafeNet eToken 7300, see Partitioning the SafeNet eToken 7300 on page 144.

> **NOTE**
>
> ♦ The SafeNet eToken 7300 initialization process always initializes the smartcard and partitions the flash drive.
>
> ♦ If partitioning settings are not set during initialization, the default partitioning settings are used.

10 To configure advanced settings, see Configuring Advanced Initialization Settings on page 114.

> **NOTE**
>
> iKey tokens do not support advanced initialization settings.

11 Click **Start**.

When the initialization process is complete, a confirmation message is displayed.

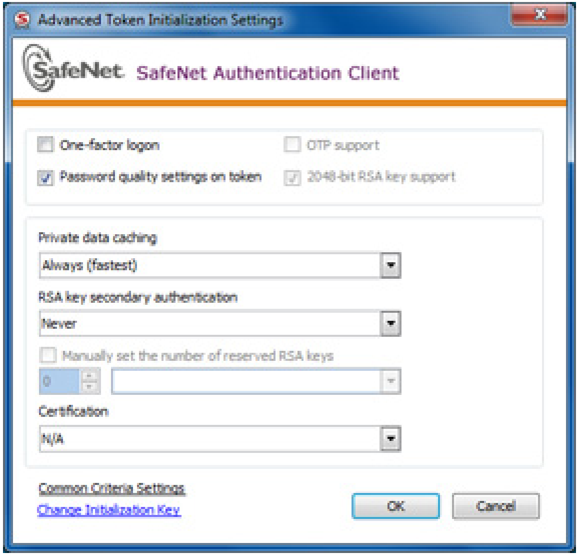
Configuring Advanced Initialization Settings

To configure advanced initialization settings:

1 Open the *Token Initialization* window.
See Configuring Initialization Settings on page 110.

2 Click **Advanced Settings**.

The *Advanced Token Initialization Settings* window opens.



Advanced Token Initialization Settings

SafeNet Authentication Client

□ One-factor logon

□ OTP support

☑ Password quality settings on token

☑ 2048-bit RSA key support

Private data caching: Always (fastest)

RSA key secondary authentication: Never

□ Manually set the number of reserved RSA keys: 0

Certification: N/A

3 Complete the fields as follows:

Field	Description
One-factor logon	Default: disabled. When one factor logon is enabled, only the presence of the token is required to log on to applications. The Token Password is not required.
Password quality settings on token	Default: enabled Select to keep password quality requirements on the token device.
OTP Support	Default: disabled Select to enable OTP support (on compatible tokens).
2048-bit RSA key support	Default: enabled Select to enable 2048-bit RSA key support (on compatible tokens).
Private data caching	Default: Always (fastest) To enhance performance, SafeNet Authentication Client caches public information stored on the token. This option defines when private information (excluding private keys on the token) can be cached outside the token. Select one of the following options: ♦ Always (fastest): Private information is always cached in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed. ♦ While user is logged on: Private information is cached outside the token as long as the user is logged on to the token. Once the user logs out, all the private data in the cache is erased. ♦ Never: Private information is not cached.

Field (Cont.)	Description (Cont.)
RSA key secondary authentication	Default: Never An authentication password may be set for an RSA key. Depending on how this option is set, in addition to having the token and knowing its Token Password, accessing the RSA key may require knowing the password set for that particular key. Having a password for the key is known as *secondary authentication*. Select one of the following: ♦ Always ♦ Always prompt user ♦ Prompt user on application request ♦ Never ♦ Token authentication on application request For an explanation of these options, see Setting the RSA Key Secondary Authentication Field on page 118. If the token was initialized as Common Criteria and the secondary authentication *Always*, *Always prompt user* or *Prompt upon application reques*t, then the secondary authentication setting cannot be changed to *Never* or *Token authentication on application request*. This limitation applies to Common Criteria certificates only.
Manually set the number of reserved RSA keys	Default: disabled Set the number of reserved RSA keys to reserve space in the token memory. This ensures that there will always be memory available for keys.

Field (Cont.)	Description (Cont.)
Certification	Default: N/A Select the certification type for formatting the token. Select one of the following options: ♦ N/A: None ♦ FIPS: Federal Information Processing Standards is a US government approved set of standards designed to improve the utilization and management of computer and related telecommunication systems ♦ Common Criteria: an international standard for computer security certification
Change Initialization Key (link)	The initialization key protects against accidental initialization and requires a separate password to be entered before initialization can occur.
Common Criteria Settings (link)	If *Certification* is set to **Common Criteria**, click this button to set the certificate import PIN and the maximum number of certificates for which to reserve space on the token.

4 You can do the following:

- To change the token initialization key, see Changing the Token Initialization Key on page 122.
- To define the Common Criteria settings, see Configuring Common Criteria Settings on page 125.

5 To return to the *Token Initialization* window, click **OK**.

Setting the RSA Key Secondary Authentication Field

The following table explains the options for the RSA key secondary authentication setting.

RSA Key Secondary Authentication settings

Setting	Description	
Always	Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.	
	If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password. When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.	If the user clicks Cancel, RSA key generation fails.

RSA Key Secondary Authentication settings

Setting	Description	
Always prompt user	Every time an RSA key is generated, the user is prompted to create a secondary password for accessing the key.	
	If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password. When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.	If the user clicks Cancel, the RSA key is generated without a secondary password. When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.

RSA Key Secondary Authentication settings

<table>
<tr><th>Setting</th><th colspan="3">Description</th></tr>
<tr><td rowspan="2">Prompt user on application request</td><td colspan="2">When using an RSA key generation application that requires secondary passwords for strong private key protection (such as Crypto API with a user protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user is prompted to create a secondary password for accessing the RSA key.</td><td rowspan="2">When using applications that do not require secondary passwords for strong private key protection, the RSA key is generated without a secondary password.
When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.</td></tr>
<tr><td>If the user clicks OK, the RSA key is generated, and the password entered becomes the new key's secondary password.
When using the certificate, the user must authenticate once using the Token Password. For each operation that requires the RSA key, the user must authenticate using the secondary password.</td><td>If the user clicks Cancel, RSA key generation fails.</td></tr>
<tr><td>Never</td><td colspan="3">Secondary passwords are not created for new RSA keys.
When using the certificate, the user must authenticate once using the Token Password. No additional authentication is required for operations that require the RSA key.</td></tr>
</table>

RSA Key Secondary Authentication settings

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">Token authentication on application request</td><td colspan="2">Secondary passwords are not created for new RSA keys.
When using the certificate, the user must authenticate once using the Token Password.</td></tr>
<tr><td>When using an RSA key generated by an application that requires secondary passwords for strong private key protection (such as Crypto API with a user protected flag, or the PKCS#11 CKA_ALWAYS_AUTHENTICATE attribute), the user must authenticate using the Token Password for each operation that requires the RSA key.</td><td>When using an RSA key that was not generated by an application that requires secondary passwords for strong private key protection, no additional authentication is required for operations that require the RSA key.</td></tr>
</table>

Changing the Token Initialization Key

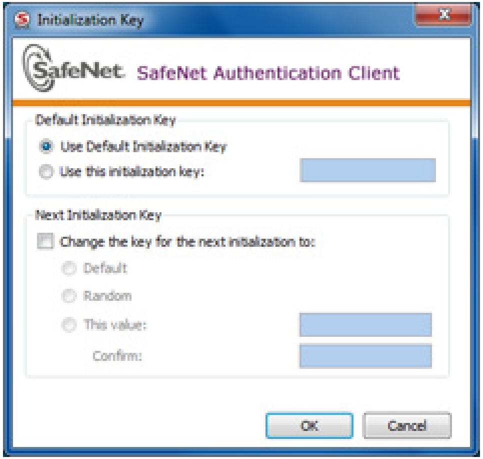
Change the Initialization Key to protect against accidental token initialization in the future. If the Initialization Key is changed from the factory-set default value, the user will be required to open the *Initialization Key* window and enter the key during future initialization of the token.

iKey tokens do not support token Initialization Keys.

To change the Token Initialization Key:

1. Open the *Advanced Settings* window.
   See Configuring Advanced Initialization Settings on page 114.
2. Click **Change Initialization Key**.

   The *Initialization Key* window opens.


Initialization Key
SafeNet
SafeNet Authentication Client
Default Initialization Key
● Use Default Initialization Key
○ Use this initialization key:
Next Initialization Key
□ Change the key for the next initialization to:
○ Default
○ Random
○ This value:
Confirm:
OK
Cancel

3 Complete the fields as follows:

Field	Description
Use default initialization key	Select this option if the Initialization Key was not changed from its default during the previous token initialization. The factory-set default is used as the key for the current token initialization.
Use this initialization key	Enter the Initialization Key configured in the *This Value* field during the previous token initialization.

Change the key for the next initialization to:	♦ **Default:** Revert to the factory-set default so that the user is not required to enter an Initialization Key during subsequent token initializations. ♦ **Random:** If selected, it will never be possible to re-initialize the token. ♦ **This Value:** Select and confirm a unique key. During subsequent token initializations, the user must enter this key in the *Use this Initialization Key* field.

4 Click **OK** to return to the *Advanced Token Initialization Settings* window.

Configuring Common Criteria Settings

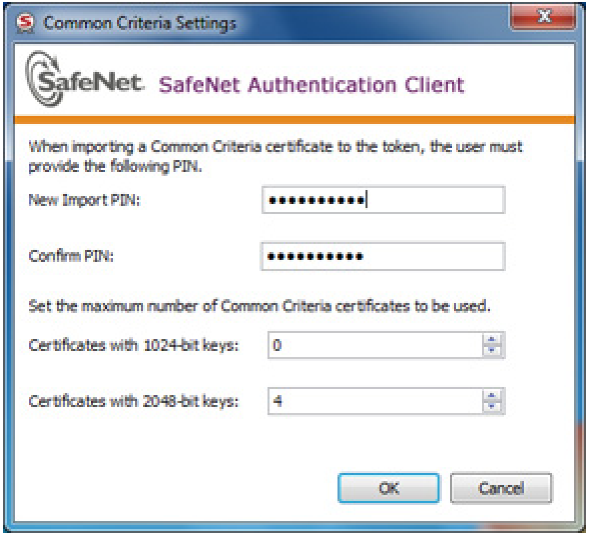
When the selected certification type is **Common Criteria**, set the certificate import PIN and the maximum number of certificates for which to reserve space on the token.

> **NOTE**
> This section is relevant only to tokens that are Common Criteria supported.

To define the Common Criteria settings:

1. Open the *Advanced Settings* window.
   See Configuring Advanced Initialization Settings on page 114.
2. In the *Certification* field, select **Common Criteria**.
3. Click **Common Criteria Settings**.

   The *Common Criteria Settings* window opens.



Common Criteria Settings

SafeNet Authentication Client

When importing a Common Criteria certificate to the token, the user must provide the following PIN.

New Import PIN: ••••••••••

Confirm PIN: ••••••••••

Set the maximum number of Common Criteria certificates to be used.

Certificates with 1024-bit keys: 0

Certificates with 2048-bit keys: 4

4 Complete the fields as follows:

Field	Description
Import PIN, Confirm PIN	Define and confirm a PIN that must be entered when a Common Criteria certificate is imported to the token. The minimum PIN length is 4 characters. The default value is **1234567890**.

Certificates with 1024-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 1024-bit keys that will be imported to the token. Select a number within the range 0 -16.
Certificates with 2048-bit keys	To reserve adequate space on the token, set the maximum number of Common Criteria certificates with 2048-bit keys that will be imported to the token. Select a number within the range 1- 16.

5 Click **OK** to return to the *Configuring Advanced Initialization Settingss* window.

5 SafeNet eToken Virtual

SafeNet Authentication Client supports the SafeNet eToken Virtual line of products. This includes SafeNet eToken Virtual and eToken Rescue tokens.

> **TIP**
> To obtain a SafeNet eToken Virtual file, contact your administrator.

In this chapter:

Overview of SafeNet eToken Virtual Products

SafeNet Authentication Client supports tokens from the SafeNet eToken Virtual family. These tokens are stored as files on your computer or on an external storage device.

The following types of software tokens are available:

- **SafeNet eToken Rescue:** provides a solution when a staff member loses or damages their token when away from the office. A SafeNet eToken Rescue is a read-only token which functions for a limited period of time. You cannot import certificates to it.
- **SafeNet eToken Virtual:** performs all the functions of an eToken NG-OTP. It can store the same data, including eToken Single Sign-On (SSO) profiles and key pairs and certificates. Its configuration may enable it to support OTP generation.

  A SafeNet eToken Virtual is “locked” to a particular computer or storage device, such as a flash drive. This means that it can be used only on the computer or storage device on which it was enrolled.
- **SafeNet eToken Virtual Temp**: identical to a SafeNet eToken Virtual, but its certificates become invalid after a pre-defined time period.

Connecting a SafeNet eToken Virtual

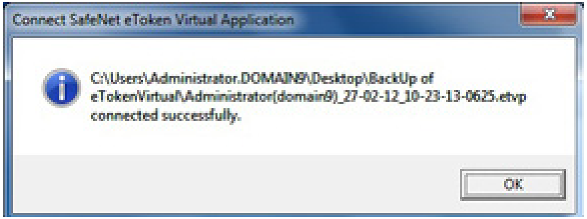
To use your SafeNet eToken Virtual product as a token, connect its file to SafeNet Authentication Client.

Under certain conditions, the token is connected automatically. See Using a SafeNet eToken Virtual on an External Storage Device on page 139.

To connect a SafeNet eToken Virtual token from the file:

1 Double-click the SafeNet eToken Virtual (.etvp) or eToken Rescue (.etv) file.

The SafeNet eToken Virtual or eToken Rescue connects to the computer and displays a confirmation message.



C:\Users\Administrator.DOMAIN9\Desktop\BackUp of eTokenVirtual\Administrator(domain9)_27-02-12_10-23-13-0625.etvp connected successfully.

2 Click **OK**.

To use SafeNet Authentication Client Tools to connect a SafeNet eToken Virtual:

3. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
4. Do one of the following:
   - In the left pane, select the **Tokens** node.
     In the right pane, click the **Connect SafeNet eToken Virtual** icon

   - In the left pane, right-click the **Tokens** node, and select **Connect SafeNet eToken Virtual** from the shortcut menu.
5. Navigate to the SafeNet eToken Virtual file (*.etvp) or eToken Rescue file (*.etv), and double-click it.

   The SafeNet eToken Virtual product is connected.

Disconnecting or Deleting a SafeNet eToken Virtual Product

For security purposes, disconnect your SafeNet eToken Virtual or SafeNet eToken Rescue from its connected reader when you are not using it.

Under certain conditions, the token is disconnected automatically. See Using a SafeNet eToken Virtual on an External Storage Device on page 139.

When your SafeNet eToken Virtual product is no longer required, disconnect and also delete it. For example, if your SafeNet eToken Rescue temporarily replaced a lost token, disconnect and delete it when you receive a permanent replacement token.

To disconnect or delete a SafeNet eToken Virtual product:

1 To use the Simple View to disconnect, do the following:

   a Open SafeNet Authentication Client Tools *Simple View.*
   See Opening the Simple View on page 20.

   b In the left pane, select the required SafeNet eToken Virtual or eToken Rescue token.

   c In the right pane, select **Disconnect SafeNet eToken Virtual** (or **Disconnect SafeNet eToken Rescue**).

   d Continue with step 3.

2 To use the Advanced View to disconnect, do the following:

a Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

b Do one of the following:

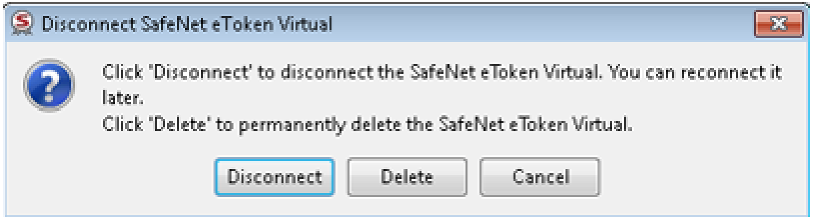
- In the left pane, select the node of the required SafeNet eToken Virtual or eToken Rescue token.
  In the right pane, click the **Disconnect SafeNet eToken Virtual** icon:

  ⏏

- In the left pane, right-click the node of the required SafeNet eToken Virtual or eToken Rescue token, and select **Disconnect** from the shortcut menu.

c Continue with step 3.

3 The *Disconnect SafeNet eToken Virtual* window opens.



Click 'Disconnect' to disconnect the SafeNet eToken Virtual. You can reconnect it later.
Click 'Delete' to permanently delete the SafeNet eToken Virtual.

4 Do one of the following:

- To keep the SafeNet eToken Virtual or eToken Rescue file on the computer or device for later use, click **Disconnect**.
  Only the token connection to SafeNet Authentication Client is disconnected. It can be reconnected later. See Connecting a SafeNet eToken Virtual on page 130.
- To disconnect the token from SafeNet Authentication Client, and also remove the SafeNet eToken Virtual or eToken Rescue file from the computer, click **Delete**.
  After a SafeNet eToken Virtual or eToken Rescue is deleted, it cannot be reconnected later. A new file must be installed before it can be connected.

Using a SafeNet eToken Virtual to Replace a Lost Token

To use a SafeNet eToken Virtual or eToken Rescue to replace a lost token, the SafeNet eToken Virtual or SafeNet eToken Rescue must be enrolled using SafeNet Authentication Manager.

For more information, refer to the SafeNet Authentication Manager documentation.

Unlocking a SafeNet eToken Virtual

If you enter an incorrect password more than a pre-defined number of times, the SafeNet eToken Virtual will become locked. To unlock the token, See Unlocking a Token by the Challenge-Response Method on page 60, or See Unlocking a Token by an Administrator on page 96.

NOTE

The number of times that a SafeNet eToken Virtual can be unlocked can be limited to a specific amount. If this number is exceeded, the SafeNet eToken Virtual becomes unusable. This function is not available for a SafeNet eToken Rescue.

Generating a One-Time Password (OTP)

The *Generate OTP* function is available only if a SafeNet eToken Virtual or eToken Rescue, with the OTP feature activated, is stored on your computer.

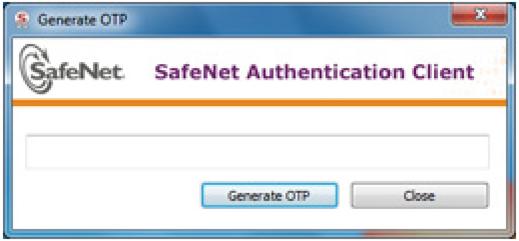
To generate an OTP:

1. Right-click the SafeNet Authentication Client tray icon.

   The SafeNet Authentication Client tray menu opens.

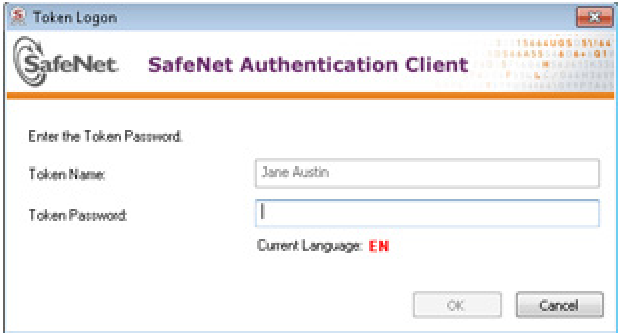
2. Select **Generate OTP**.

   The *Generate OTP* window opens.



3. Click **Generate OTP**.

   The *Token Logon* window opens.



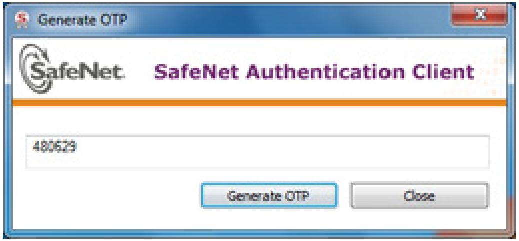
Enter the Token Password.

Token Name: Jane Austin

Token Password:

Current Language: EN

4 Enter the Token Password, and click **OK**. The OTP is displayed in the *Generate OTP* window.



480629

5 Use the OTP to authenticate yourself to your application.

NOTE

Depending on your SAC configuration, you may need to include other secure information, e.g. OTP PIN or Windows password.

6 Close the *Generate OTP* window.

Using a SafeNet eToken Virtual on an External Storage Device

The operating system automatically connects a SafeNet eToken Virtual product when all of the following conditions are met:

- The SafeNet eToken Virtual file is locked to an external storage device, such as a flash drive.
- The file is located in the `eTokenVirtual` folder on the storage device.
- The storage device is connected to the computer.

When the storage device is removed from the computer, the operating system automatically disconnects the SafeNet eToken Virtual that was automatically connected.

If the SafeNet eToken Virtual is located on an external storage device in a location other than the `eTokenVirtual` folder, you will need to connect the SafeNet eToken Virtual manually. See Connecting a SafeNet eToken Virtual on page 130.

Before removing the storage device, you will need to disconnect the SafeNet eToken Virtual manually. See Disconnecting or Deleting a SafeNet eToken Virtual Product on page 132. Otherwise, the SafeNet eToken Virtual will be displayed in SafeNet Authentication Client as a token with corrupted data. See Token Icons on page 22.

Using an Emulated SafeNet eToken Virtual

Certain applications that work with smart card readers require the SafeNet eToken Virtual to emulate the action of the smart card reader. To use a SafeNet eToken Virtual product with such applications, you must use an emulated SafeNet eToken Virtual.

Typically, the emulated SafeNet eToken Virtual is locked to an external storage device.

By default, the emulated SafeNet eToken Virtual cannot be locked to your computer's hard drive, as this can cause a malfunction of the Windows logon. This occurs because the Windows logon process cannot deal with multiple smart card readers. However, if you want to work with the SafeNet eToken Virtual located on the hard drive, the administrator can configure SafeNet Authentication Client to support this.

It is important to disconnect the emulated SafeNet eToken Virtual when you have finished the session, so that the computer reverts to working with the default reader.

6 SafeNet eToken 7300

SafeNet eToken 7300 is a certificate-based authentication solution that securely stores data and applications on up to 64GB of encrypted flash memory.

In this chapter:

Connecting a SafeNet eToken 7300

After connecting a SafeNet eToken 7300, the Windows *AutoPlay* window opens.

You can access SafeNet’s default ISO file by performing either one of the following:

- Run Launcher.exe
- Open folder to view files
- Click **My Computer** and open the specific drive

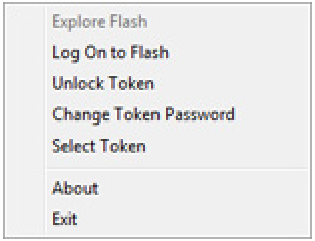
The SafeNet Flash Drive icon is displayed in the Windows task bar.

To open the SafeNet Flash Drive tray icon menu:

1 Right-click the Flash Drive icon.

The Flash Drive shortcut menu opens.

> **NOTE**
> This shortcut menu is also available when right-clicking the SAC Monitor tray icon.



2 Select the required menu item.

The following functions can be launched from the shortcut menu:

- Explore flash
- Log on to flash/Log off from flash (Available if the token is configured with a password protected Flash partition)
- Unlock token (See *Unlocking a Token by the Challenge-Response Method* on page 60, or See *Unlocking a Token by an Administrator* on page 96)
- Change Token Password (See *Changing the Token Password* on page 56)
- About
- Exit

Partitioning the SafeNet eToken 7300

SAC 8.2 supports partitioning the SafeNet eToken 7300 by dividing the token's flash drive into a DVD partition and a user storage partition.

Either one of the following can be performed on the SafeNet eToken 7300:

- **Initialize and partition:** The initialization process deletes the data from the smartcard and flash drive (user storage). New data is written to the smartcard.

  The partitioning process allows you to configure the flash drive partitioning settings, and divide the flash drive into a DVD partition and a user storage partition.

- **Partition without initializing:** The flash drive is divided into a DVD and user storage partition without deleting and resetting the smartcard’s contents.

To partition the SafeNet eToken 7300:

1 Do one of the following:

  ♦ To initialize and partition the SafeNet eToken 7300:

    i Open the *Token Initialization* window.
    See Configuring Initialization Settings on page 110.

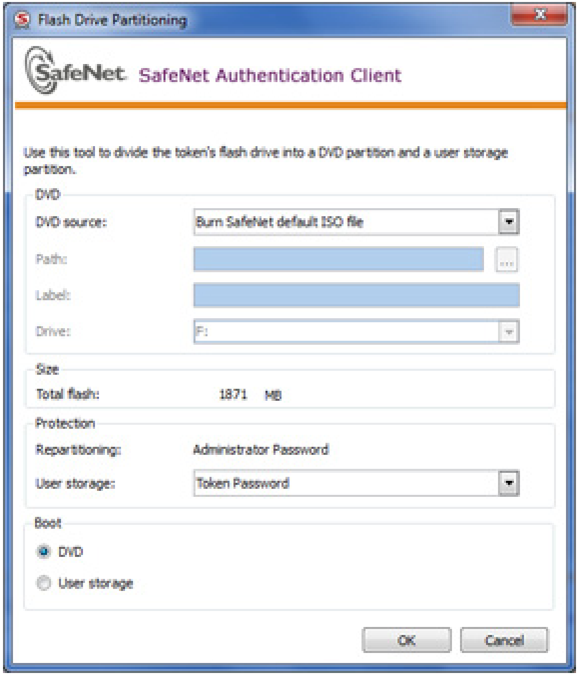
    ii Click the **Partitioning Settings** link.

  ♦ To partition the SafeNet eToken 7300 without initialization:

i Open SafeNet Authentication Client Tools *Advanced View.*
See *Opening the Advanced View* on page 25.

ii In the left pane, right-click the node of the required SafeNet eToken 7300, and select **Partition Flash Drive** from the shortcut menu.

The *Flash Drive Partitioning* window opens.



Use this tool to divide the token's flash drive into a DVD partition and a user storage partition.

DVD

DVD source: Burn SafeNet default ISO file

Path:

Label:

Drive: F:

Size

Total flash: 1871 MB

Protection

Repartitioning: Administrator Password

User storage: Token Password

Boot

● DVD

○ User storage

NOTE

When partitioning the SafeNet eToken 7300 without initialization, a Start button is displayed at the bottom of the Flash Drive Partitioning window.

2 In the DVD Source drop-down list, select either one of the following options:

- **Burn SafeNet default ISO file:** burns the SafeNet default ISO file located in the SAC folder
- **Burn ISO file:** burns an ISO file located elsewhere on the computer
- **Copy from ROM drive:** copies files from the selected CD ROM drive
- **Copy from folder:** copies an entire folder from the computer

> **NOTE**
> Selecting the *Burn ISO file* or *Copy from folder* option activates the *Path* field.
> Selecting the *Copy from ROM drive* option activates the *Drive* field.
> Selecting the *Copy from folder* option activates the *Path* and *Label* fields.

The *Flash Drive Partitioning window* also includes the following details:

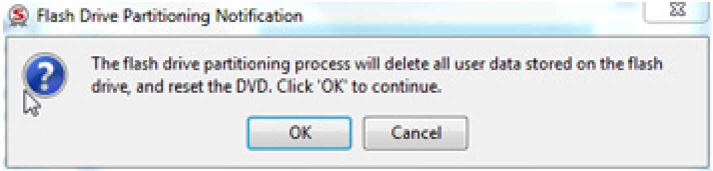
- **Size:** total size of the flash memory (DVD + user storage)
- **Protection:** password protection requirements for partitioning and for accessing the user storage.

> **NOTE**
> Partitioning will be password protected only if the Administrator Password is set in the *Token initialization window.*

- **Boot -** select whether to load the DVD contents or user storage contents when connecting the SafeNet eToken 7300.

3 Click **Start**.

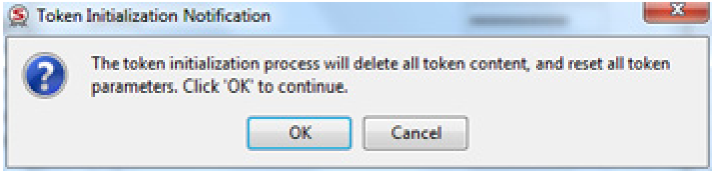
- When partitioning without initialization, the *Flash Drive Partitioning Notification* window opens.



Flash Drive Partitioning Notification

The flash drive partitioning process will delete all user data stored on the flash drive, and reset the DVD. Click 'OK' to continue.

- When initializing the token, the *Token Initialization Notification* window opens.

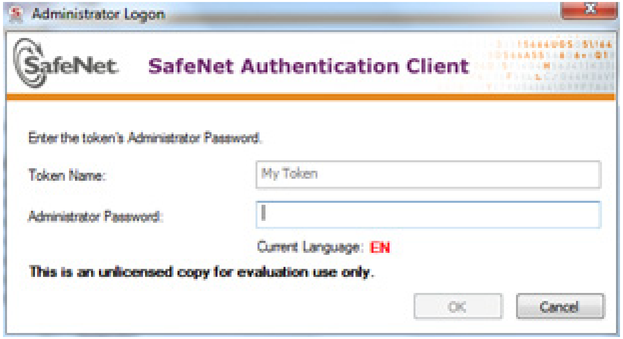


Token Initialization Notification

The token initialization process will delete all token content, and reset all token parameters. Click 'OK' to continue.

4 Click **OK**.

If the partitioning process is password protected, the *Administrator Logon* window opens.



Administrator Logon

SafeNet Authentication Client

Enter the token's Administrator Password.

Token Name: My Token

Administrator Password:

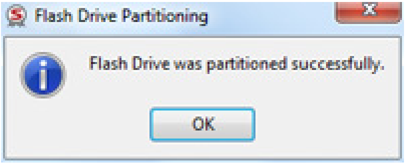
Current Language: EN

This is an unlicensed copy for evaluation use only.

Enter the token's *Administrator Password*.

5 Click **OK**.

When the partitioning process is complete, a confirmation message is displayed.



Flash Drive Partitioning

Flash Drive was partitioned successfully.

6 Click **OK.**

7 Client Settings

Client Settings are parameters that are saved to the computer and apply to all tokens that are initialized on the computer after the settings have been configured. Use token settings to determine behavior that applies to a specific token. See Chapter 8 Token Settings.

In this chapter:

Setting Password Quality

The *Password Quality* feature enables the administrator to set certain complexity and usage requirements for Token Passwords.

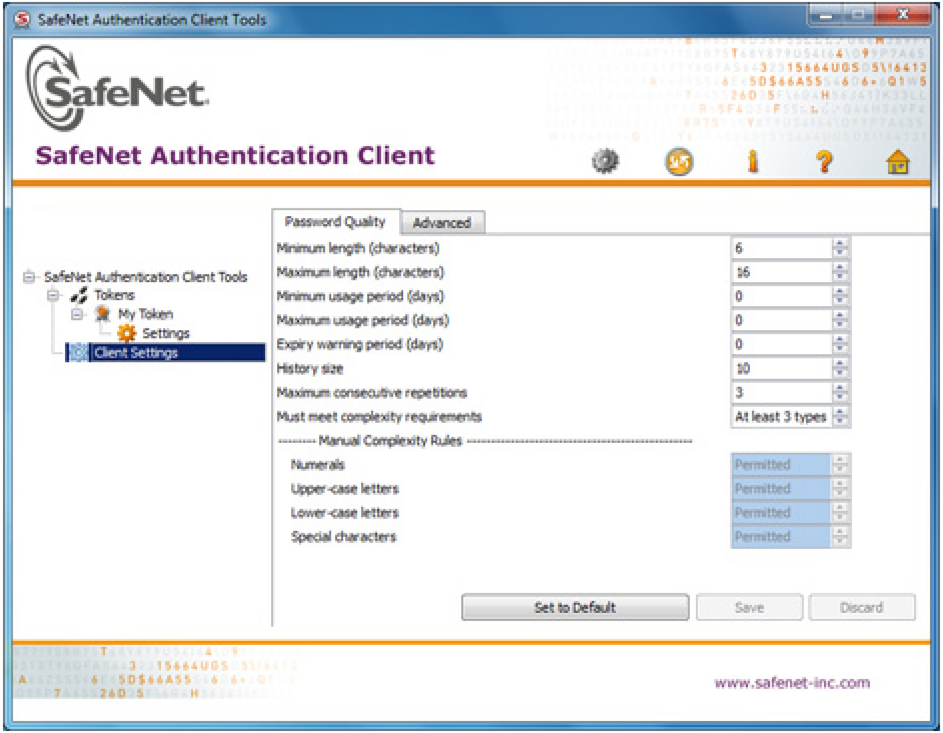
NOTE

The Token Password is an important security measure in safeguarding your company's private information. The best passwords are at least eight characters long, and include upper-case and lower-case letters, punctuation marks, and numbers appearing in a random order.

To set the Password Quality:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Password Quality** tab.

   The *Password Quality* tab opens.



Minimum length (characters)	6
Maximum length (characters)	16
Minimum usage period (days)	0
Maximum usage period (days)	0
Expiry warning period (days)	0
History size	10
Maximum consecutive repetitions	3
Must meet complexity requirements	At least 3 types
-------- Manual Complexity Rules --------	
Numerals	Permitted
Upper-case letters	Permitted
Lower-case letters	Permitted
Special characters	Permitted

4 Do one of the following:

♦ Change the password quality settings, and click **Save.**

TIP

The Client Settings password quality settings are configured the same way as the Token Password quality settings. See Setting Token Password Quality on page 168

- To ignore your changes, click **Discard.**
- To apply SafeNet Authentication Client's default settings, click **Set to Default.**

NOTE

When entering a value in the *Expiry warning period* field, you must make sure that a value is also entered in the *Maximum usage period* field. If no value is entered in the *Maximum usage period* field, an error message appears.

Copying User Certificates to a Local Store

SafeNet Authentication Client operations often require certificates, private keys, and public keys.

Private keys should always be stored securely on the token. Certificates should also be stored on the token as this enables mobility, ensuring that the certificate will be readily available when using the token on a different computer.

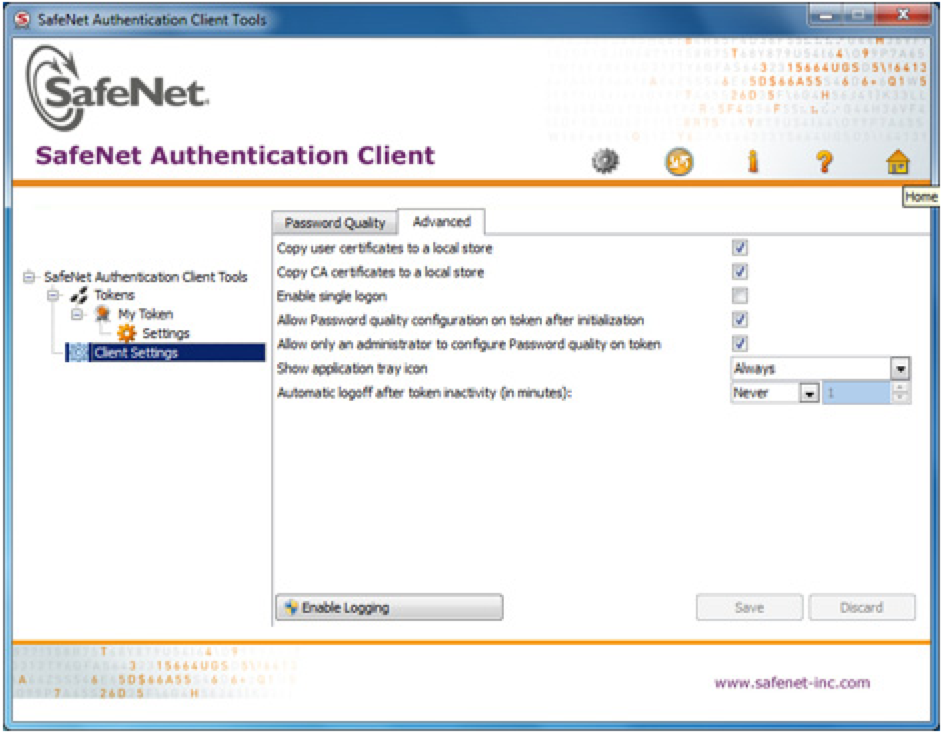
Use SafeNet Authentication Client settings to control the action of automatically copying all user certificates to the certificate store upon token connection.

This option is selected by default.

To copy user certificates to a local store:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.

The *Advanced* tab opens.



SafeNet Authentication Client Tools

SafeNet Authentication Client

- SafeNet Authentication Client Tools
  - Tokens
    - My Token
      - Settings
  - Client Settings

Password Quality | Advanced

Copy user certificates to a local store	☑
Copy CA certificates to a local store	☑
Enable single logon	□
Allow Password quality configuration on token after initialization	☑
Allow only an administrator to configure Password quality on token	☑
Show application tray icon	Always
Automatic logoff after token inactivity (in minutes):	Never 1

4 Select **Copy user certificates to a local store**.

5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Copying CA Certificates to a Local Store

CA certificates can be downloaded to a token. When the token is connected to the computer, one or more of these CA certificates may not be on the computer. In such a case, the CA certificate may be loaded onto the computer.

This option is selected by default.

To copy CA certificates to a local store:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Copy CA certificates to a local store**.

NOTE
It is possible that another window from Microsoft opens asking if you wish to continue this action. This is standard Microsoft operating procedure because the action to be undertaken may affect computer security. If you want to copy the CA certificate, click Yes.

5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Enabling Single Logon

When single logon is enabled, users can access multiple applications with only one request for the Token Password during each computer session. This alleviates the need for the user to log on to each application separately.

> **NOTE**
>
> Setting the single logon using SAC Tools will not include a Windows Logon on the single logon process. This must be configured by the system administrator.

This option is disabled by default.

To enable single logon:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Enable Single Logon.**
5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes click, **Discard.**
6. To activate the single logon feature, log off from the computer and log on again.

Allowing Password Quality Configuration on Token after Initialization

> **NOTE**
> This feature is not supported by iKey tokens.

The *Allow password quality configuration on token after initialization* option determines whether the password quality parameters on the token may be changed after initialization.

To enable password quality configuration after initialization:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Select **Allow password quality configuration on token after initialization.**
5. Do one of the following:
   - ♦ To save your changes, click **Save.**
   - ♦ To ignore your changes, click **Discard.**

Allowing Only an Administrator to Configure Password Quality on Token

The *Allow only an administrator to configure password quality on token* option determines whether the password quality parameters on the token may be changed after initialization by the administrator only, and not by the user.

This option is selected by default.

To define who can configure password quality on token:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. Do one of the following:
   - To enable configuration by the administrator only, select **Allow only an administrator to configure password quality on token***.*
   - To enable configuration by the user also, clear **Allow only an administrator to configure password quality on token***.*

5 Do one of the following:

- To save your changes, click **Save.**
- To ignore your changes, click **Discard.**

Showing SafeNet Authentication Client Tray Icon

You can determine whether the SafeNet Authentication Client tray icon is displayed.

To show the SafeNet Authentication Client tray icon:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *Show application tray icon* drop-down list, select one of the following:
   - **Never**: The tray icon is never displayed
   - **Always**: The tray icon is always displayed
5. Do one of the following:
   - To save your changes, click **Save.**
   - To ignore your changes, click **Discard.**

Defining Automatic Logoff

You can determine whether tokens are automatically logged off following a period of token inactivity, even if the tokens are not disconnected.

After a token is logged off, the user must enter the Token Password again before the token contents can be accessed.

To define the automatic logoff setting:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *Automatic logoff after token inactivity* drop-down list, select one of the following:
   - **Never**: The Token Password must be entered once, and the token remains logged on as long as it remains connected.
   - **Always**: The Token Password must be entered each time the token contents are accessed.
   - **After**: The Token Password must be entered if the number of minutes set in the text box has passed since the last token activity.
     Set the number of minutes in the text box (1 - 254).

5 Do one of the following:

- To save your changes, click **Save.**
- To ignore your changes, click **Discard.**

Enabling Logging

The logging feature creates a log of SafeNet Authentication Client activities.

> **NOTE**
> You must have administrator privileges to use the logging feature.

The log files are located at: `C:\WINDOWS\Temp\eToken.log`

To activate the logging feature:

1. Open SafeNet Authentication Client Tools *Advanced View*.
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.
3. In the right pane, select the **Advanced** tab, and click **Enable Logging.**

> **NOTE**
> You must restart your machine for the settings to take effect.

To disable the logging feature:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, select **Client Settings**.

3 In the right pane, select the **Advanced** tab, and click **Disable Logging**.

8 Token Settings

Configurations set in the selected token's *Settings* tab determine behavior that applies to the specific token.

For configurations set in *Client Settings*, that apply the settings to all tokens that are initialized after the settings have been configured, see Chapter 7 Client Settings.

In this chapter:

Setting Token Password Quality

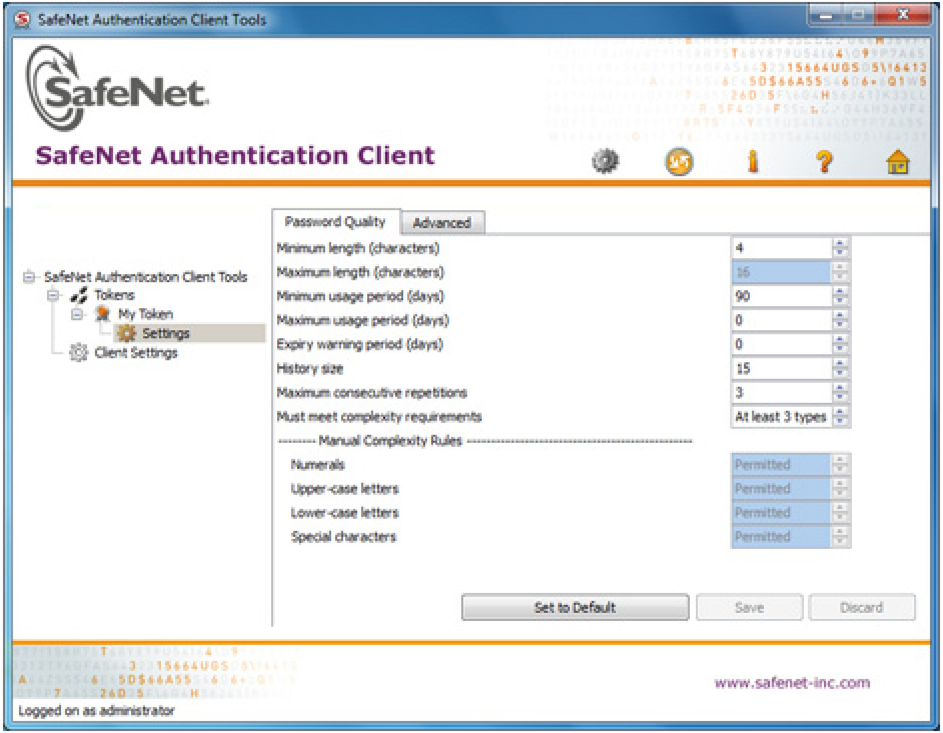
If a token is initialized after Token Password quality parameters are set for the token, all future Token Password are automatically checked against these parameters to determine the password's level of acceptability.

If a token was initialized in early eToken PKI Client versions (RTE), no password policy is stored on the token.

If an iKey token was initialized previously in BSec Client, its password quality parameters will continue to be supported by SafeNet Authentication Client.

To set password quality for a token:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Password Quality** tab.
4. The *Password Quality* tab opens.



Minimum length (characters)	4
Maximum length (characters)	16
Minimum usage period (days)	90
Maximum usage period (days)	0
Expiry warning period (days)	0
History size	15
Maximum consecutive repetitions	3
Must meet complexity requirements	At least 3 types

-------- Manual Complexity Rules --------

Numerals	Permitted
Upper-case letters	Permitted
Lower-case letters	Permitted
Special characters	Permitted

Logged on as administrator

5 Enter the password quality parameters as follows:

Password Quality Parameter	Description
Minimum length (characters)	Default: 6 characters

Password Quality Parameter	Description (Cont.)
Maximum length (characters)	Default: 16 characters
Maximum usage period (days)	The maximum period, in days, before which the password must be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks (7 days), even though the period is displayed in days. For example, if the period is displayed as less than a week, say 6 days, iKey regards it as a week. If the period is more than two weeks, say 15 days, iKey regards it as three weeks.
Minimum usage period (days)	The minimum period before the password can be changed. Default: 0 (none) For iKey devices, the periods are rounded up to periods of weeks. See row above for more information.
Expiration warning period (days)	Defines the number of days before the password expires that a warning message is shown. Default: 0 (none)
History size	Defines how many previous passwords must not be repeated. Default: For eToken devices - 10 For iKey devices - 6

Password Quality Parameter	Description (Cont.)
Maximum consecutive repetitions	The maximum number of repeated characters that is permitted in the password. Default: 3 This feature is not supported by iKey devices.
Must meet complexity requirements	Determines the complexity requirements that are required in the Token Password. ♦ **At least 2 types:** a minimum of 2 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced. ♦ **At least 3 types:** a minimum of 3 complexity rules (out of the 4 shown in the Manual Complexity fields) are enforced (Default). ♦ **None:** Complexity requirements are not enforced. ♦ **Manual:** Complexity requirements, as set manually in the *Manual Complexity* settings, are enforced.
Manual complexity rules	For each of the character types (**Numerals, Upper-case letters, Lower-case letters,** and **Special characters**) select one of the following options: ♦ **Permitted -** Can be included in the password, but is not mandatory (Default). ♦ **Mandatory -** Must be included in the password. ♦ **Forbidden -** Must not be included in the password. **Note:** The **Forbidden** option is not supported by iKey devices.

6 Do one of the following:

- To save your changes, click **Save.**
- To ignore your changes, click **Discard.**
- To apply SafeNet Authentication Client’s default settings, click **Set to Default.**

Setting Private Data Caching Mode

NOTE
This feature is not supported by iKey devices.

In SafeNet Authentication Client, public information stored on the token is cached to enhance performance. This option defines when private information (excluding private keys on the eToken PRO / NG OTP / smart card) can be cached outside the token.

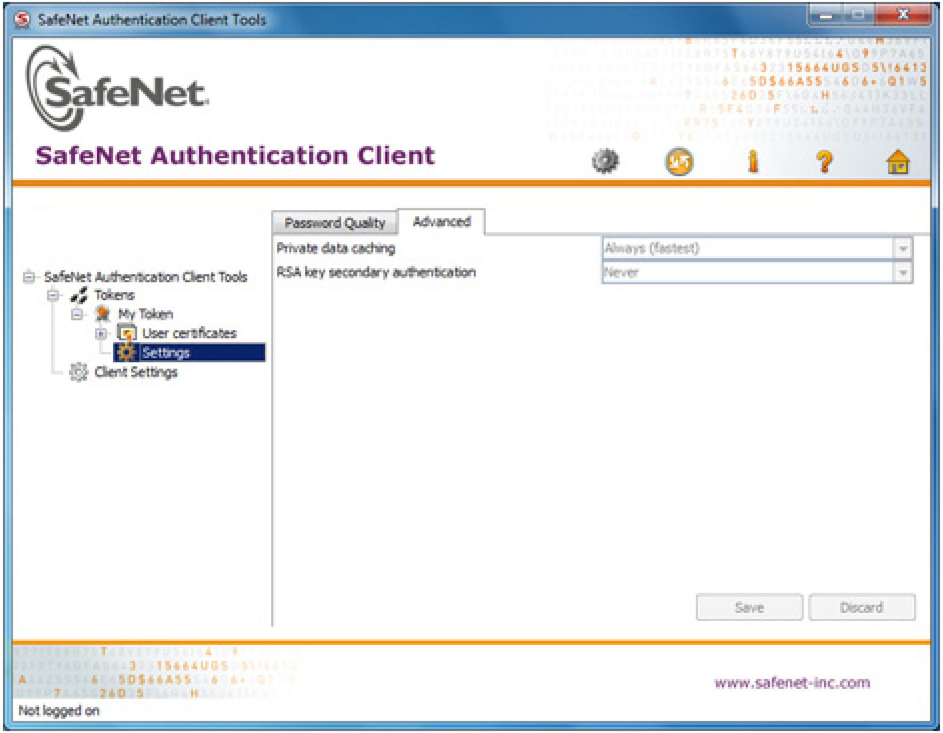
To set private data caching mode:

1 Open SafeNet Authentication Client Tools *Advanced View.*
See Opening the Advanced View on page 25.

2 In the left pane, expand the node of the required token, and select **Settings**.

3 In the right pane, select the **Advanced** tab.

The *Advanced* tab opens.



Private data caching: Always (fastest)

RSA key secondary authentication: Never

4 In the *Private data caching* field, select one of the following options:

Option	Description
Always (fastest)	Always caches private information in the application memory. This enables fast performance, as certain information is cached on the host machine. However, this option is less secure than if no cache is allowed.
While user is logged on	Caches private data outside the token as long as the user is logged on to the token. Once the user logs off, all the private data in the cache is erased.
Never	Does not cache private data.

5 Do one of the following:

- ♦ To save your changes, click **Save.**
- ♦ To ignore your changes, click **Discard.**

Setting RSA Key Secondary Authentication

> **NOTE**
> This feature is not supported by iKey devices.

An authentication password may be set for an RSA key. Depending on how this option is set, in addition to having the token and knowing its Token Password, accessing the RSA key may require knowing the password set for that particular key.

This option defines the policy for using this secondary authentication of RSA keys.

To set RSA key secondary authentication:

1. Open SafeNet Authentication Client Tools *Advanced View.*
   See Opening the Advanced View on page 25.
2. In the left pane, expand the node of the required token, and select **Settings**.
3. In the right pane, select the **Advanced** tab.
4. In the *RSA key secondary authentication* field, select one of the following:
   - Always
   - Always prompt user
   - Prompt user on application request
   - Never
   - Token authentication on application request

> **NOTE**
> For an explanation of these options, see Chapter 4:Setting the RSA Key Secondary Authentication Field, on page 118

5 Do one of the following:

- To save your changes, click **Save.**
- To ignore your changes, click **Discard.**

9 Licensing

Import a SafeNet license for your SafeNet Authentication Client installation.

In this chapter:

Viewing and Importing Licenses

SafeNet Authentication Client installations that do not have a SafeNet license can be used for evaluation only, and a message is displayed on all logon windows.

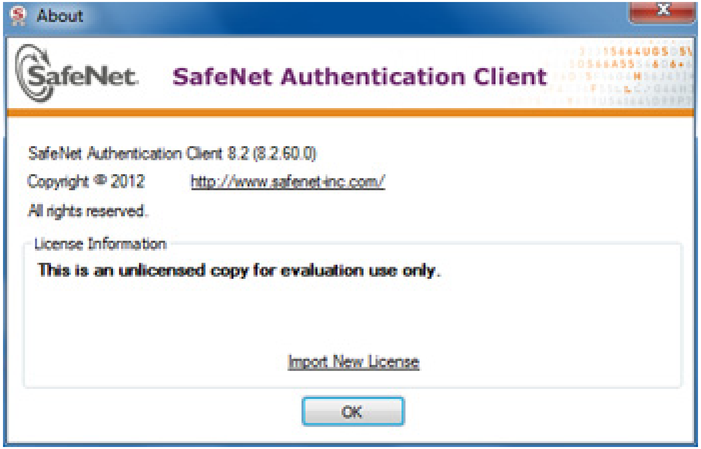
You can view your licenses and import new ones using the SafeNet Authentication Client *About* window.

To view and import licenses:

1 Do one of the following:

- Right-click the SafeNet Authentication Client tray icon, and from the shortcut menu, select **About**.
- Open SafeNet Authentication Client Tools. See Opening the Advanced View on page 25. On the toolbar, click the **About** icon.

The *About* window opens, displaying your license information in the *License Information* box.



SafeNet Authentication Client 8.2 (8.2.60.0)

Copyright © 2012 http://www.safenet-inc.com/

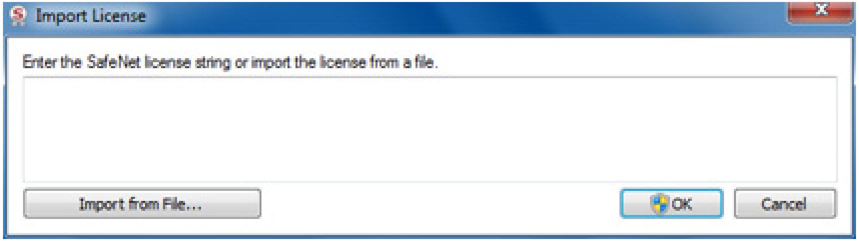
All rights reserved.

License Information

This is an unlicensed copy for evaluation use only.

2 To import a new license, select **Import New License**.

The *Import License* window opens.



Enter the SafeNet license string or import the license from a file.

3 Do one of the following:

- If the SafeNet license box is automatically filled, click **OK**.
- Copy your new SafeNet license string to the license box, and click **OK**.
- Click **Import from File**, browse to the file containing your license, open it to copy its contents to the license box, and click **OK**.

  The *About* window opens, displaying your updated license information in the *License Information* box.